Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Ulisses Simas Huguenim

SEGURANÇA EM REDES CABEADAS: Implementação de Controle de Admissão ao Meio em Redes de Larga Escala

Rio de Janeiro

2007

Ulisses Simas Huguenim

SEGURANÇA EM REDES CABEADAS:
Implementação de Controle de Admissão ao Meio em Redes de Larga Escala

Monografia apresentada para obtenção do título de Especialista de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Prof. João Carlos Peixoto de Almeida da Costa, Mestrado em Informática, UFRJ, Brasil

Rio de Janeiro

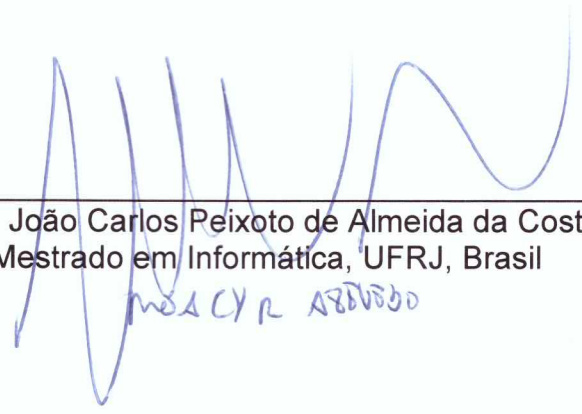
2007

Ulisses Simas Huguenim

SEGURANÇA EM REDES CABEADAS:
Implementação de Controle de Admissão ao Meio em Redes de Larga Escala

Monografia apresentada para obtenção do título de Especialista de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em março de 2007.



p/ Prof. João Carlos Peixoto de Almeida da Costa
Mestrado em Informática, UFRJ, Brasil

Dedico este trabalho a minha esposa que através do seu amor, me faz sentir amado, colocando brilho nos meus olhos e resplandecendo meu sorriso.

AGRADECIMENTOS

Agradeço a Deus pela oportunidade de realizar este curso, por estar aqui fazendo esta pesquisa e por saber que Ele cuida de mim.

RESUMO

HUGUENIM, Ulisses Simas. **SEGURANÇA EM REDES CABEADAS: Implementação de Controle de Admissão ao Meio em Redes de Larga Escala.** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2006.

O padrão IEEE 802.1x implementa controles de acesso a rede diretamente nas portas dos switchs. Mas existem alguns problemas que encontramos na hora de implementar esta tecnologia em ambientes de larga escala. Por se tratar de redes extensas, surgem muitas exceções, como servidores espalhados pela empresa, cascateamento de switchs não documentados, utilização de recursos da rede por inúmeros consultores externos, entre outros. Este trabalho tem como finalidade ser um guia prático de configuração do padrão 802.1x, mostrando alguns problemas encontrados e quais soluções adotadas.

ABSTRACT

HUGUENIM, Ulisses Simas. **SEGURANÇA EM REDES CABEADAS: Implementação de Controle de Admissão ao Meio em Redes de Larga Escala.** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2006.

The IEEE standard 802.1x implements network access controls directly in the switch ports. But some problems appear when we implement this technology in environments of wide scale. Treating with extensive nets, many exceptions, as Computer Servers spread by the company, switchs not registered, use of resources of the net for innumerable external consultants appear, among others. This work has as purpose to be a practical guide of configuration of the standard 802.1x, showing to some joined problems and which adopted solutions.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

CHAP	Challenge-handshake authentication protocol
EAP	Extensible Authentication Protocol
FAT	File Allocation Table
FDDI	Fiber distributed data interface
GUI	Graphical User Interface
HOWTO	Termo utilizado na área da informática para designar um manual
IAS	Internet Authentication Service
IDS	Intrusion-detection system
IEEE	Institute of Electrical and Electronics Engineers
IPS	Intrusion-prevention system
MD5	Message-Digest algorithm 5
NTFS	New Technology File System
OTP	One-time password
PEAP	Protected Extensible Authentication Protocol
PPP	Point-to-Point Protocol
RADIUS	Remote Authentication Dial In User Service
TCP/IP	Transmission Control Protocol (TCP) Internet Protocol (IP)
TI	Tecnologia da Informação
TLS	Transport Layer Security
UDP	User Datagram Protocol
VPN	virtual private network

SUMÁRIO

1 INTRODUÇÃO

1.1 OBJETIVOS

O Controle de Admissão ao Meio é padronizado pelo IEEE 802.1x podendo ser utilizado em redes cabeadas Ethernet ou em redes sem fio. Com este controle, um dispositivo de rede não pode enviar quadros à rede até que ocorra a autenticação com sucesso, evitando assim que equipamentos não autorizados à organização tentem utilizar os recursos de TI sem a devida autorização e conhecimento da equipe de TI. Ainda podem ser utilizadas políticas que forcem a atualização de patchs de segurança e vacinas anti-vírus antes de liberar o acesso ao meio.

No decorrer dessa monografia será detalhado o funcionamento do padrão IEEE 802.1x em redes cabeadas, detalhando a configuração dos componentes necessários (estações de trabalho, switchs e servidores) e as dificuldades encontradas no momento da implantação.

1.2 RELEVÂNCIA

A perda de dados resultante de um ataque malicioso ao sistema de um computador pode ser algo devastador para uma organização. A fim de ajudar a proteger os sistemas e os dados das empresas contra as constantes ameaças de códigos maliciosos usados em worms, vírus, e ataques maliciosos, é fundamental que sejam implementadas medidas de segurança para ajudar a reduzir a exposição a esses problemas. E a forma como o IEEE 802.1x funciona, deixando somente os equipamentos conhecidos gerarem tráfego na rede, torna a rede bem mais segura, pois dessa forma se conhece 100% dos equipamentos que estão conectados a esta e que devem ser protegidos com os outros meios de segurança já conhecidos, como anti-vírus, atualizações de segurança do sistema operacional/aplicativos, entre outras coisas.

2 REFERENCIAL TEÓRICO

2.1 CONSIDERAÇÕES INICIAIS

Neste capitulo será apresentada a fundamentação teórica para o entendimento do desenvolvimento deste trabalho, o qual baseia-se na implantação do Controle de Admissão ao Meio utilizando o padrão IEEE 802.1x.

Serão listados os tipos de rede existentes, e em mais detalhes a rede Ethernet, que é a mais usada nas redes locais e que será estudo da nossa pesquisa. Será descrito como ocorreu a evolução deste padrão de rede e como o Controle de Acesso ao Meio demonstra ser mais uma evolução deste padrão tornando-a mais segura.

Em paralelo a evolução das redes, será descrita a evolução dos sistemas operacionais utilizados nas estações de trabalho que também fazem parte do processo para a implantação do Controle de Admissão ao Meio.

Finalmente, serão abordadas as tecnologias que apoiam a implementação do 802.1x, como autenticação através do Active Directory, servidor Radius e o protocolo EAP.

2.2 TIPOS DE REDES LOCAIS

As principais tecnologias de redes locais cabeadas disponíveis são Ethernet, Token ring e FDDI.

Uma das diferenças entre essas tecnologias é o conjunto de regras que cada uma usa para introduzir e remover dados do cabo de rede, sendo esse procedimento chamado de método de acesso. Quando os dados trafegam na rede, esses métodos de acesso regulam o fluxo do tráfego.

2.3 REDE ETHERNET

2.3.1 Cabeamento

Existem basicamente três tipos diferentes de cabos de rede: os cabos de par trançado (que são os mais comuns), os cabos de fibra óptica (usados principalmente em links de longa distância) e os cabos coaxiais, usados em redes locais antigas. Estes cabos foram usados quando as redes locais estavam surgindo e as mesmas trabalhavam isoladamente. Ainda não existia a Internet e a preocupação com

segurança se concentrava em controlar os vírus que estavam contidos nos disquetes.

2.3.2 Hub

"O Hub é indicado para redes com poucos terminais de rede, pois o mesmo não comporta um grande volume de informações passando por ele ao mesmo tempo devido sua metodologia de trabalho por broadcast, que envia a mesma informação dentro de uma rede para todas as máquinas interligadas. Devido a isto, sua aplicação para uma rede maior é desaconselhada, pois geraria lentidão na troca de informações.

Um hub se encontra na primeira camada do modelo OSI por não poder definir para qual computador se destina a informação, ele simplesmente a replica." (WIKIPÉDIA, HUB)

Depois das redes baseadas em cabo coaxial, surgiram as que utilizam hubs e o cabo de par-trançado. Estes equipamentos denominados hub, concentram todas as ligações dos cabos em um ponto central. Surgia então o conceito de cabeamento estruturado. Em termos de segurança, não houve nenhum ganho. Pelo contrário, as redes estavam ganhando uma maior interligação entre as mesmas e a Internet já estava fazendo parte desta interconexão. A segurança neste caso estava sendo tratada pelos equipamentos de borda, denominados firewall. Mas internamente não existia nenhum tipo de proteção contra os ataques a partir da rede interna, podendo qualquer pessoa que entrasse na empresa e plugasse seu notebook num ponto da rede local, acessar os recursos disponíveis na rede.

2.3.3 Switch

"Um switch, que foi traduzido para comutador, é um dispositivo utilizado em redes de computadores para reencaminhar dados entre os diversos nós. Possuem diversas portas, assim como os hubs, e operam na camada acima dos hubs. A diferença é que segmenta a rede internamente, sendo que a cada porta corresponde um segmento diferente, o que significa que não haverá colisões entre os segmentos diferentes — ao contrário dos hubs, cujas portas partilham o mesmo domínio de colisão.

Os computadores operam semelhantemente a um sistema telefônico com linhas privadas. Nesse sistema, quando uma pessoa liga pra outra a central telefônica as conectará em uma linha dedicada, possibilitando um maior número de conversações simultâneas.

Um comutador opera na camada 2 (ligação ou enlace de dados) encaminhando os pacotes de acordo com o endereço MAC de destino e é destinado a redes locais para segmentação. Porém, existem atualmente comutadores que operam juntamente na camada 3 (camada de rede), herdando algumas

propriedades dos roteadores (routers). Estes dispositivos chamam-se switch-routers.” (WIKIPÉDIA, SWITCH)

Agora na era dos switchs, as redes já estão fortemente interligadas em altíssimas velocidades. Vários dispositivos de segurança são utilizados, principalmente nos perímetros da rede. Firewall, IDS, IPS e Anti-Spam são alguns bons exemplos. Mas internamente os switchs trazem poucos avanços no quesito segurança. Pode-se fazer o controle por endereço MAC nas portas dos switchs, controlando assim quais estações podem acessar a rede local. Mas isso só é viável em redes de pouquíssimos pontos. Em redes de larga escala, com milhares de estações e pontos de rede local, esse controle manual se torna inviável devido o excesso de trabalho que esse controle causaria e o atraso em qualquer processo que envolvesse movimentação de equipamentos dentro da empresa.

2.4 **EVOLUÇÃO DO SISTEMA OPERACIONAL DE REDE**

2.4.1 (WorkGroup) Windows 3.11

“Os sistemas operacionais Windows 3.x da família Microsoft Windows foram lançados entre 1990 e 1994. A versão 3.0 foi o primeiro sucesso amplo do Windows, permitindo que a Microsoft pudesse competir com a Apple Computer e seu sistema, o Macintosh mais a GUI Commodore Amiga.

Voltada principalmente a redes locais (LANs) propiciando maior facilidade aos usuários construírem suas próprias redes.

Pode ter sido responsável pela saída do mercado de empresas como Novell e Lantastic, que dominavam como fornecedoras de NOSes (sistemas operacionais para redes) em plataformas cliente-servidor e ponto a ponto, respectivamente.” (WIKIPÉDIA, WINDOWS 3.X)

O Windows 3.11, é da mesma época das redes interligadas pelo cabo coaxial. Foi o começo da interface gráfica e que hoje nos leva a estar a apenas um clique de sermos infectados por um vírus que recebemos por email. Esta versão trouxe a facilidade de configurarmos redes distribuídas ponto a ponto. Mas que nos trás o problema, por ser uma rede distribuída, de não termos o controle de quem está acessando quem, tornando-se uma rede muito insegura.

2.4.2 (Cliente / Servidor) Windows 98 / Windows NT

“O Windows 98 foi lançado pela Microsoft em julho de 1998, trazia como novidade a completa integração entre o sistema operacional e a Internet. A grande novidade é o suporte a múltiplos monitores e USB. Uma segunda edição, chamada de Windows 98 SE (de Second Edition) foi lançada em 1999 servia para corrigir os

bugs da versão anterior e trazia drivers e programas atualizados. Muitos usuários classificam esse sistema como um dos melhores já lançados pela Microsoft.” (WIKIPÉDIA, WINDOWS 98)

“O Windows NT foi lançado pela Microsoft com o objetivo principal de fornecer mais segurança e comodidade para ambientes corporativos, isto é, usuários de empresas e lojas. A sigla NT significa New Tecnology (nova tecnologia) e a partir de 2001 este tipo de Windows começou a ter outros nomes, ser oferecido também para usuários domésticos e começou a mudar de visual, como um exemplo o Windows XP(Windows NT 5.1). Este versão permaneceu sem popularidade até o fim da era 9x/ME, quando lançaram o Windows 2000 ou NT 5.0. Nesta edição também foi implementado a idéia de Serviços, no qual o sistema operacional trabalha a partir de serviços, tendo assim menores chances de travar, pois era possível reinicializar apenas um serviço do que a máquina por inteiro. Esta versão do Windows aceita três tipos de sistemas de arquivos:

FAT16 - Windows NT 3.xx e Windows NT 4.0;

FAT32 - Windows 2000, Windows XP e Windows 2003;

NTFS - Windows NT 4.0, Windows 2000, Windows XP e Windows 2003”. (WIKIPÉDIA, WINDOWS NT)

Nestas versões de sistemas operacionais, a base de arquivos fica centralizada no servidor e acessada via rede local pelos clientes. Já existe uma preocupação na segurança dos arquivos onde são definidas regras de acesso aos mesmos. Programas de anti-virus monitoram em “real-time” estes arquivos, tanto no servidor como nas estações. Mas ainda existe uma dificuldade na administração das estações cliente com respeito à atualização de patchs de segurança, instalação de softwares, etc. O TCP/IP passa a ser o protocolo padrão de comunicação e suas brechas de segurança passam a ser atacadas. A interconexão das redes locais propicia uma facilidade de propagação de vírus e worms através do protocolo TCP/IP.

2.4.3 (Cliente / Servidor) Windows XP / Windows 2003

- Windows XP (Cliente)

“Esta é a versão mais recente, lançada em Outubro de 2001 e é também conhecida como Windows NT 5.1. Roda em formatações FAT32 (File Allocation Table, em português: "tabela de alocação de arquivos") ou NTFS (New Tecnology File System, em português: "nova tecnologia de sistema de arquivos"). A sigla XP deriva da palavra “eXPeriência”. Uma das principais diferenças em relação às versões anteriores é quanto à interface. Trata-se da primeira mudança radical desde o lançamento do Windows 95. A partir deste Windows, surgiu uma nova interface, abandonando o antigo formato 3D acinzentado. Também é notável a incrível diferença de velocidade com quaisquer versão anterior, o suporte a Hardware também foi melhorado em relação às versões 9x.

Foi no Windows XP que os Service Packs obtiveram maior significado visto não só corrigirem falhas, mas também por adicionarem novas funcionalidades.

Em 2002 foi lançado o primeiro Service Pack, que veio corrigir e acrescentar funcionalidades ao Windows XP.

No Verão de 2004 a Microsoft lançou o segundo service pack para o Windows XP, que além de corrigir erros, introduziu um novo nivel de segurança no Windows XP quer ao nível do utilizador, quer ao nível da internet. Uma das grandes novas características está no fato de que é extremamente difícil tentar explorar uma vulnerabilidade encontrada no sistema. A segunda grande inovação foi a inclusão de uma API para criadores de antivírus que facilita não só a detecção de vírus como também ajuda o antivírus a integrar-se com o novo Security Center (Central de Segurança) disponível no painel de controle.

A Central de Segurança é onde o usuário escolhe as opções para a segurança do sistema, como as exceções do firewall (programas e/ou portas que têm acesso permitido com a Internet) e atualizações automáticas." (WIKIPÉDIA, WINDOWS XP)

- Windows 2003

"Lançado pela Microsoft em 24 de abril de 2003, o Windows Server 2003 é um sistema operacional de rede desenvolvido como sucessor do Windows 2000 Server. Em seu núcleo está uma versão do Windows XP com algumas funções desligadas para permitir um funcionamento mais estável do sistema.

Assim como o Windows 2000, este apresenta o Active Directory como principal ferramenta para a administração de uma rede. É um sistema utilizado extritamente em redes de computadores.

Esta versão trouxe novas melhorias aos serviços de rede e ao Active Directory, que agora implementa mais funcionalidades em relação ao Windows 2000 Server.

Em 30 de Março de 2005, Microsoft lança Service Pack 1 para Windows Server 2003. Entre as novidades, incluem: Security Configuration Wizard, Hot Patching, Windows Firewall e Data Execution Prevention (DEP), entre outras." (WIKIPÉDIA, WINDOWS 2003)

Já nestas versões, a preocupação com segurança está bem mais focada. Políticas de segurança podem ser replicadas a partir do servidor para todas as estações clientes. Estas versões já são preparadas para utilizar o protocolo 802.1x.

2.5 **MÉTODO DE AUTENTICAÇÃO**

2.5.1 Active Directory

"Um diretório é uma estrutura hierárquica que armazena informações sobre objetos existentes na rede. Um serviço de diretório, tal como o Active Directory® fornece os métodos para armazenar dados e para disponibilizar estes dados aos usuários e administradores. Por exemplo, o Active Directory armazena informações sobre contas de usuários, tais como nomes, números de telefone, entre outras, e permite que outros usuários autorizados, existentes na mesma rede, acessem a estas informações." (MICROSOFT, AD)

O Active Directory também é utilizado como autenticador na rede, liberando ou não o acesso de uma estação cliente, que esteja registrado no domínio. Mas ele não impede que um usuário se autentique localmente em sua estação e acesse os recursos da rede. Nessa área que o controle de acesso ao meio vai atuar, sendo que este também vai utilizar o Active Directory para autorizar o equipamento a acessar os recursos de rede, não sendo necessário assim criar mais um usuário e senha para isso, o que é uma grande vantagem.

2.5.2 Servidor Radius

"O RADIUS é usado para fornecer serviços de autenticação, autorização e estatísticas. Um cliente RADIUS (normalmente um servidor de rede dial-up, servidor VPN ou ponto de acesso sem fio) envia informações sobre o parâmetro de conexão e as credenciais de usuários no formato de mensagem RADIUS para um servidor RADIUS. O servidor RADIUS autentica e autoriza a solicitação do cliente RADIUS e envia de volta uma resposta de mensagem RADIUS. Os clientes RADIUS também enviam mensagens sobre estatísticas RADIUS para servidores RADIUS. Além disso, os padrões RADIUS oferecem suporte ao uso de proxies RADIUS. Um proxy RADIUS é um computador que encaminha mensagens RADIUS entre computadores ativados por RADIUS.

As mensagens RADIUS são enviadas como mensagens do protocolo de datagrama de usuário (UDP). A porta UDP 1812 é usada para mensagens de autenticação RADIUS e a porta UDP 1813 é usada para mensagens sobre estatísticas RADIUS. Alguns servidores de acesso de rede podem usar a porta 1645 UDP para mensagens de autenticação RADIUS e a porta 1646 UDP para mensagens sobre estatísticas RADIUS." (MICROSOFT, RADIUS)

No Controle de Acesso ao meio, o switch irá solicitar a estação uma credencial, que será repassada ao servidor RADIUS, que por sua vez irá verificar no Active Directory. Resumidamente, assim funciona o padrão 802.1x, controlando o acesso ao meio. Por se tratar de um processo crítico o momento da autenticação numa empresa, o serviço RADIUS deve ter pelo menos uma redundância.

2.5.3 EAP - Extensible Authentication Protocol

"O Protocolo de Autenticação Extensível (EAP, Extensible Authentication Protocol) expande o Protocolo Ponto a Ponto (PPP, Point-to-Point Protocol), pois permite a utilização de métodos de autenticação arbitrários que utilizam trocas de credenciais e informações de comprimentos arbitrários. O EAP foi desenvolvido em resposta à procura crescente de métodos de autenticação que utilizam dispositivos de segurança tais como cartões Smart Card, cartões de segurança e calculadoras criptográficas. O EAP proporciona uma arquitetura padrão da indústria para suportar métodos de autenticação adicionais no âmbito do PPP." (MICROSOFT, EAP)

O EAP é um “framework” de autenticação e não, um mecanismo de autenticação. O mesmo suporta cerca de 40 diferentes métodos de autenticação, como por exemplo: EAP-MD5, EAP-OTP, EAP-TLS e PEAP.

O PEAP já vem embutido nos sistemas operacionais Windows XP/2003 e no Windows 2000 SP4. Este mecanismo foi criado em conjunto pela Cisco System, Microsoft e RSA Security. É similar ao EAP-TLS, requerendo ao lado do servidor uma chave pública para criar um túnel TLS para proteger a autenticação do usuário.

2.5.4 IEEE 802.1x

“O 802.1X é projetado para trabalhar em qualquer tipo de rede: com ou sem fio. O 802.1X requer uma infra-estrutura de suporte, clientes nominais que suportem o 802.1X, switches do LAN e pontos de acesso sem fio que podem participar no 802.1X, um servidor RADIUS, e algum tipo de banco de dados de contas (como o Active Directory).

Um cliente, chamado supplicant (suplicante), faz uma conexão inicial para um authenticator (autenticador), que pode ser um switch de rede ou um ponto de acesso sem fio. O autenticador é configurado para exigir o 802.1X de todos os suplicantes e irá ignorar qualquer conexão de entrada que não se adequar. O autenticador solicita ao suplicante sua identidade, a qual ele passará adiante para o authentication server (RADIUS).

O RADIUS segue qualquer mecanismo necessário para autenticar o cliente que está entrando. Em geral, isto envolve a instalação de uma conversa EAP entre o suplicante e o servidor de autenticação (o autenticador é apenas um dispositivo de passagem aqui - proxy) e o estabelecimento de um método de autenticação dentro da conversa EAP. Note que o EAP em si não define qualquer tipo de segurança sozinho - os protocolos de identificação usados devem incorporar sua própria segurança.

Assim que o RADIUS tenha autenticado o suplicante, o suplicante pode se comunicar na rede atrás do autenticador (lembre-se, este é o switch LAN ou o ponto de acesso sem fio). Apesar de um autenticador ter uma porta de rede física, pense nele como tendo duas "portas virtuais". O tráfego dos suplicantes autenticados passa pela porta controlada, que bloqueia o tráfego de suplicantes não autenticados. Durante o processo de autenticação o autenticador deve se comunicar com o servidor RADIUS, o que ocorre através da porta não controlada. Após a autenticação de um suplicante, a porta controlada transita para um estado conectado para aquele suplicante.” (MICROSOFT, 802.1x)

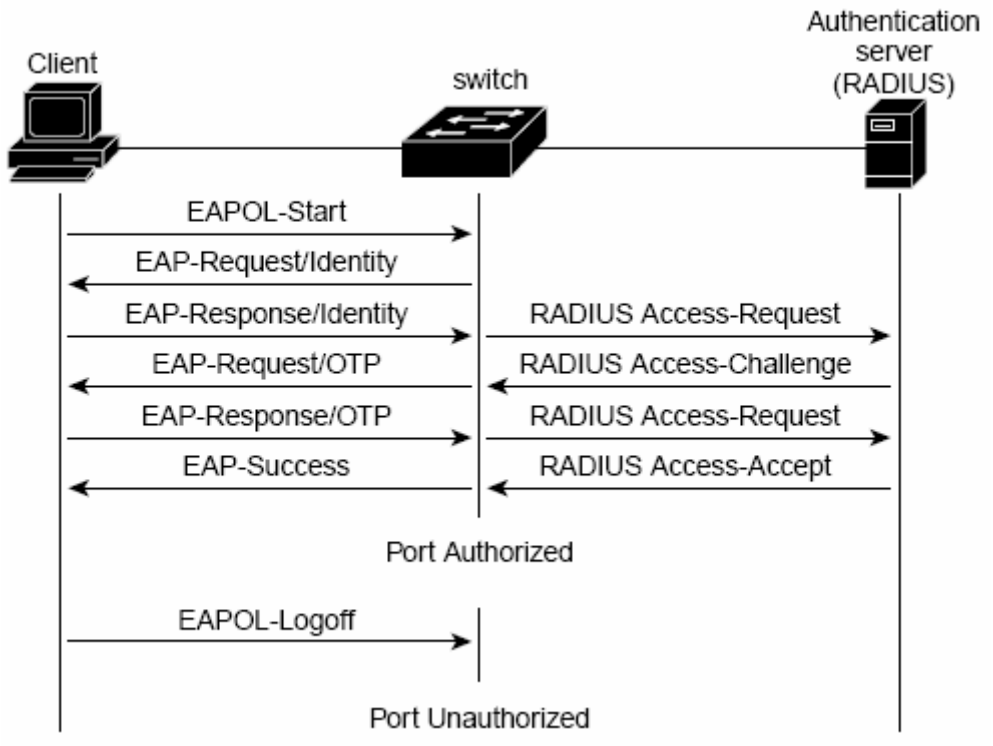


Figura 1 – Troca de mensagens (Cliente x Switch x Radius)

Na Figura 1 vemos dois processos ilustrados. A primeira ilustração mostra o momento em que a estação cliente foi ligada. Tanto o switch como a estação podem inicializar esta autenticação. Neste caso a estação começou enviando um EAPOL-Start e se fosse o caso do switch começar, este já enviaria diretamente o EAP-Request/Identity para a estação e não haveria a mensagem EAPOL-Start.

Em seguida a estação cliente, responde a solicitação com o EAP-Response/Identity informando sua identidade (usuário que será utilizado para a autenticação no Radius)

O servidor RADIUS recebe o access-request e então envia ao switch o access-challenge (desafio), momento em que o switch envia a estação cliente o EAP-Request/OTP.

A estação recebendo o Request/OTP, responde o desafio com o Response/OTP, que é a resposta do desafio lançado pelo servidor RADIUS.

Finalmente, após o servidor RADIUS receber a resposta do desafio através do Access-Request, o mesmo envia um Access-Accept para o switch. Quando então o switch passa a porta do switch para o estado de “Port Authorized” e envia a mensagem de EAP-Success para a estação informando que a autenticação foi feita com sucesso.

O segundo processo ilustra o momento de uma desconexão do cliente, quando este envia um EAPOL-Logoff, e no mesmo instante o switch passa a porta para o estado de “Port Unauthorized”, bloqueando o tráfego naquela porta.

3 DESENVOLVIMENTO

3.1 CONSIDERAÇÕES INICIAIS

Será demonstrado como estações de trabalho em um domínio do Active Directory, utilizam o mesmo usuário do domínio para fazer a autenticação na porta do switch, como são tratadas as exceções e quais as dificuldades encontradas. Para isso, diversos exemplos de configuração e captura de telas dos equipamentos serão mostrados, tornando assim este objeto de estudo um guia prático para a implantação de políticas de autenticação na porta do switch utilizando o padrão 802.1x

Serão utilizados os seguintes softwares e equipamentos:

- Servidor Windows 2003 com o Active Directory, Certification Authority e Radius instalado;
- Estações de trabalho utilizando Windows XP
- Switch Enterasys 6H302-48, 7H4382-49 e B2H124-48.
- Switch Cisco 2950

O porte da empresa onde se esta sendo feito este trabalho de pesquisa, tem cerca de 3.000 pontos de rede e tem como planejamento a implantação de uma política de autenticação utilizando o padrão 802.1x em médio prazo.

Estações com o sistema operacional Linux não são utilizados por essa empresa e por isso não fazem parte deste estudo. Mas verificamos que este sistema operacional já vem com o cliente 802.1x e a configuração do mesmo está disponível na Internet através de HOWTOs.

Este trabalho será dividido em três partes: configuração dos switchs, configuração do servidor Radius e, por fim, configuração da estação de trabalho.

3.2 CONFIGURAÇÃO DOS SWITCHS

A configuração dos switchs da Enterasys e Cisco são fáceis de realizar e bem documentados pelo manual dos fabricantes. Um problema encontrado é que não há uma padronização nos pacotes que os switchs enviam ao servidor Radius, diferenciando de acordo com o modelo do switch ou até mesmo entre os mesmos modelos com “firmwares” diferentes. Isso dificulta a configuração do servidor Radius, que será detalhada adiante. Devido a este problema, o ideal é que sejam atualizados todos os switchs para a última versão disponibilizada pelo fabricante,

sendo isto uma primeira dificuldade encontrada numa rede que opera em regime 24x7, visto que essa atualização gera a necessidade de reiniciar o equipamento e consequentemente uma parada de alguns minutos nas estações atendidas pelo switch que se está sendo atualizado.

Abaixo segue a captura de telas do Ethereal quando o switch está se comunicando com o servidor Radius para ilustrar o problema citado acima, referente a diferença dos pacotes entre os switch e o servidor radius.

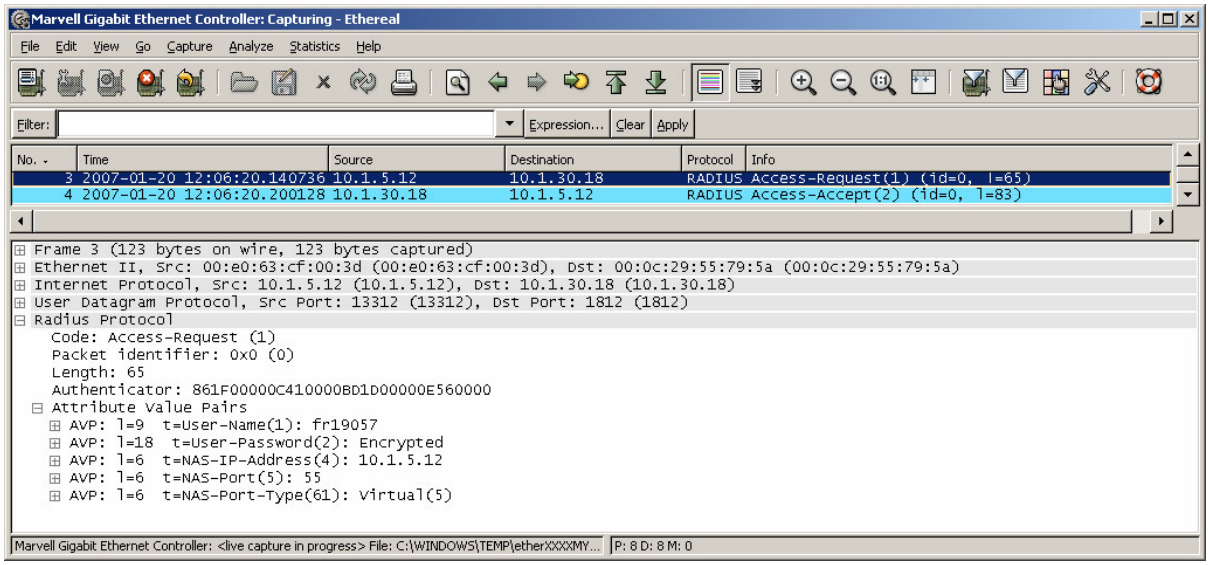


Figura 2 – Captura de pacotes com o firmware do switch desatualizado

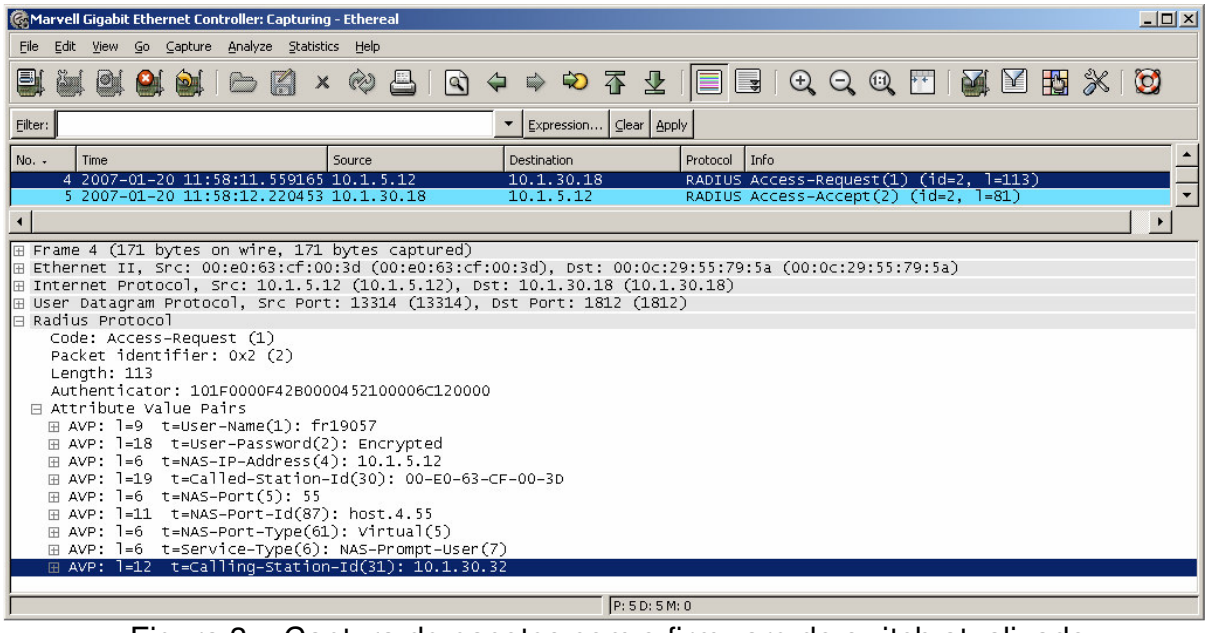


Figura 3 – Captura de pacotes com o firmware do switch atualizado

De acordo com a relação de switchs que foi listada acima, os firmwares e IOS dos switchs foram atualizados com as últimas versões disponíveis de acordo com as capacidades dos switchs, conforme a tabela abaixo:

Tabela 1 – Relação dos Modelos de Switchs

Switch	**Firmware/IOS**
6H	05.08.18
7H	05.26.05
B2	03.01.24
2950	12.1(22)EA8a

Outra dificuldade encontrada numa empresa de grande escala, é a diversidade de switchs encontrados, pois sendo diferente a configuração em cada um deles, exige do técnico um maior conhecimento e mais tempo para testar todos os modelos em um ambiente de testes, antes de colocar em produção. Além disso, exige também que a empresa tenha um maior número de equipamentos em laboratório, pois há a necessidade que se tenha um de cada modelo pelo menos.

3.2.1 Configuração dos parâmetros do Servidor Radius

Será demonstrado abaixo como é feita à configuração nos switchs para que os mesmo possuam as configurações necessárias para autenticar os usuários no servidor Radius. Os principais itens de configuração são: endereço ip do servidor Radius, frase secreta que será configurada no servidor Radius e porta TCP para estabelecimento de conexão.

3.2.1.1 Switch Enterasys B2

Abaixo segue a seqüência de comandos que deve ser aplicada através do telnet no B2.

Tabela 2 – Configurações do Radius no Switch B2

set radius enable	Habilita o serviço de Radius no switch
set radius retries 2	Número de tentativas de conexão do switch com o servidor Radius
set radius timeout 3	Tempo (em segundos) para estabilizar contato com o servidor Radius
set radius server 1 [ipservidorradius] 1812 [chave secreta] realm any	Especifica o endereço ip do primeiro servidor Radius, a chave secreta e Habilita o switch para utilizar o servidor Radius no momento da autenticação do gerenciamento do mesmo (telnet ou ssh) e também na política de acesso as portas do switch

3.2.1.2 Switch Enterasys 7H

Abaixo segue a seqüência de comandos que deve ser aplicada através do telnet no 7H. Apesar de ser muito parecida com o B2, ela tem uma particularidade que os comandos “set radius server” e set radius realm” funcionam separadamente.

Tabela 3 – Configurações do Radius no Switch 7H

set radius enable	Habilita o serviço de Radius no switch
set radius retries 2	Número de tentativas de conexão do switch com o servidor Radius
set radius timeout 3	Tempo (em segundos) para estabilizar contato com o servidor Radius
set radius server 1 [ip servidor radius] 1812 [chave secreta]	Especifica o endereço ip do servidor 1º Radius e a chave secreta
set radius realm any	Habilita o switch para utilizar o servidor Radius no momento da autenticação do gerenciamento do mesmo (telnet ou ssh) e também na política de acesso as portas do switch

3.2.1.3 Switch Enterasys 6H

A configuração do switch 6H é feita através de menus, como visto na captura de tela abaixo.

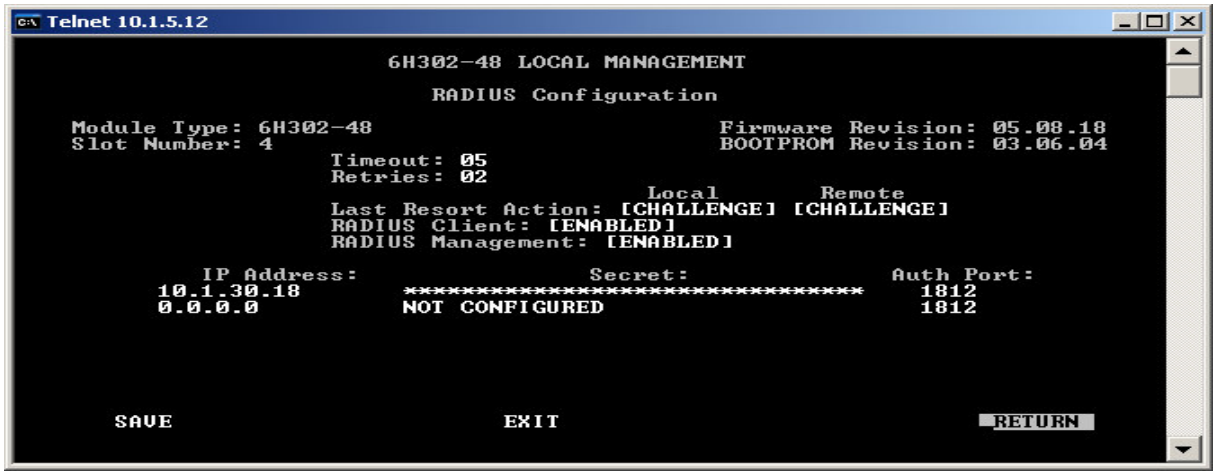


Figura 4 – Tela do Switch 6H configurando o Radius

As opções configuradas são as seguintes:

Tabela 4 – Configurações do Radius no switch 6H

Timeout	Tempo(em segundos) para estabilizar contato com o servidor Radius
Retries	Número de tentativas de conexão do switch com o servidor Radius
Last Resort Action	Configura o switch tanto para acesso via telnet/ssh ou console local no caso de falha na autenticação do acesso de gerenciamento do mesmo para o método de autendicação local. Está opção não se aplica a autenticação dot1x na porta de acesso do switch.
Radius Client	Habilita o cliente Radius no switch
Radius Management	Habilita o Radius para ser utilizado no acesso ao gerenciamento do switch via telnet/ssh
Ip Address	Informa o endereço IP do servidor Radius, a chave secreta e a porta TCP a ser utilizada.

3.2.1.4 Switch Cisco 2950

Podemos observar que os parâmetros de configurações são praticamente os mesmos em todos os equipamentos, diferenciando somente a sintaxe de como implementá-los. No caso do switch Cisco 2950, exemplificamos somente um comando, deixando os outros parâmetros associados ao Radius com seus valores “Default”, mas isso não indica que o Cisco não possa mudar estes valores “Defaults”, por outros valores que sejam mais adequadas de acordo com as condições da rede.

Tabela 5 – Configurações do Radius no switch Cisco 2950

Radius-server host [ip servidor radius] key [chave secreta]	Específica qual o IP do servidor Radius e a chave secreta

3.2.2 Configuração dos parâmetros do dot1x

Será demonstrado abaixo como é feita à configuração nos switchs para que os mesmo solicitem a autenticação às estações no momento em que o switch detecte que há portadora na porta ethernet do mesmo. Os principais itens de configuração são: habilitar o dot1x globalmente no switch e habilitar o dot1x na porta específica do switch em que se deseja esta funcionalidade.

3.2.2.1 Switch Enterasys B2

Abaixo segue a seqüência de comandos que deve ser aplicada através do telnet no B2.

Tabela 6 – Configurações do dot1x no switch B2

set dot1x enable	Habilita a autenticação 802.1X no switch
set eapol enable	Habilita a autenticação por porta com o servidor Radius
set eapol auth-mode forced-auth fe.1.1	Desabilita a autenticação por porta na porta especifica

No caso do switch B2 foi necessário alterar o parâmetro (set dot1x auth-config txperiod 3600), pois o switch estava reautenticando a estação de 30 em 30 segundos mesmo estando desabilitada a opção da reautenticação, como ilustrado na figura abaixo. Por isso foi alterado para 3600 segundos/60 minutos. Na verdade isso é um bug deste firmware do B2, pois na versão anterior não acontecia este reautenticação de 30 em 30 segundos.

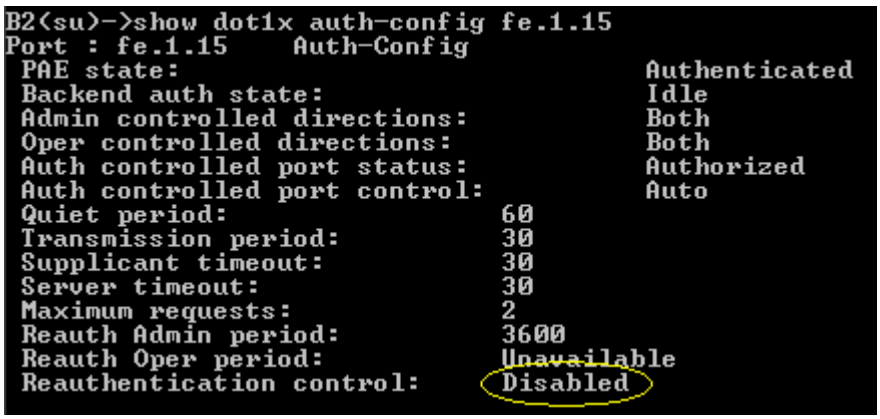


Figura 5 – Tela do switch B2 com bug na reautenticação

Segue abaixo a captura da tela do Ethereal mostrando a reautenticação de 30 em 30 segundos que causava um link down / link up na placa de rede da estação de trabalho no momento da reautenticação e em alguns momentos também falhou a

reautenticação, o que causou o link down de 30 segundos até que ocorresse a nova reautenticação. Outro problema gerado por essa reautenticação constante é o tráfego gerado na rede e a sobrecarga do servidor Radius.

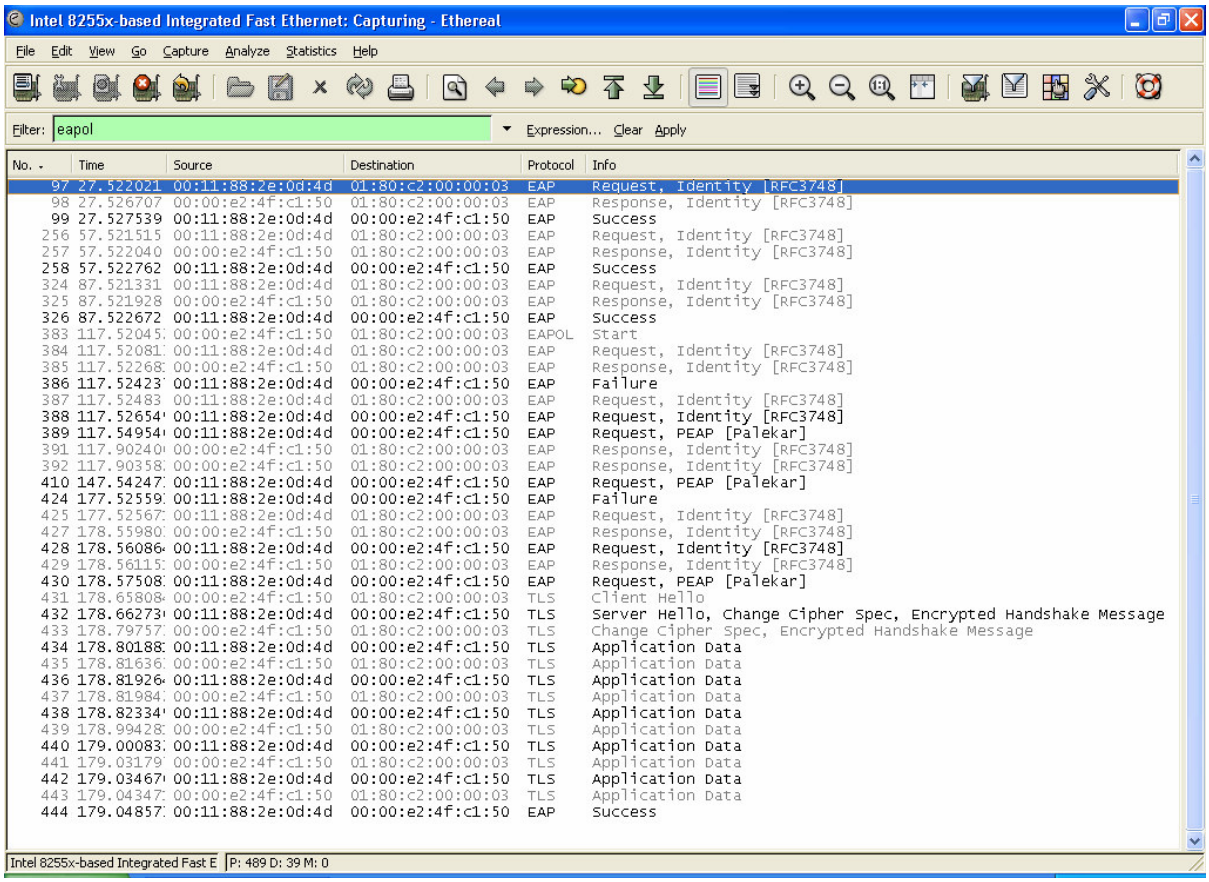


Figura 6 – Tela do Ethereal mostrando a reautenticação de 30 em 30 segundos

3.2.2.2 Switch Enterasys 7H

Abaixo segue a seqüência de comandos que deve ser aplicada através do telnet no 7H.

Tabela 7 – Configurações do dot1x no switch 7H

set dot1x enable	Habilita de forma global no switch o método de autenticação dot1x
set dot1x auth-config authcontrolled-portcontrol forced-auth fe.5.1	Desabilita o dot1x em uma porta específica

Uma dica importante é alterar primeiro a configuração das portas para “Forced Auth” antes de habilitar de forma global. E depois então mudar, porta por porta, para “Auto” (set dot1x auth-config authcontrolled-portcontrol auto fe.5.1), caso se queira utilizar o 802.1x nas portas específicas, pois se as estações ainda não estiverem

configuradas para autenticação pelo 802.1x, as mesmas perderam conexão no exato momento que for habilitada de forma global no switch o dot1x.

3.2.2.3 Switch Enterasys 6H

Na tela mostrada abaixo, habilita-se o switch globalmente para a autenticação nas portas do switch utilizando o método EAP.

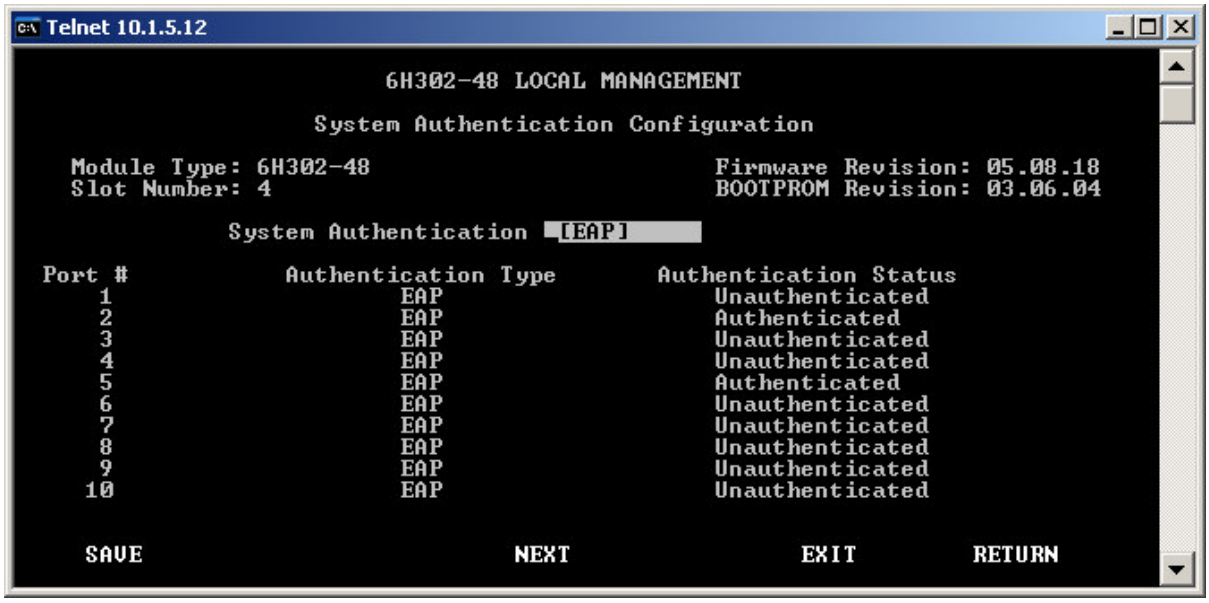


Figura 7 – Tela do switch 6H habilitando de forma global o dot1x

Assim como no 7H, vale a dica para primeiro alterar a configuração das portas para “Forced Auth” antes de fazer a alteração do método acima. Outra dica importante, é que mesmo as portas estando configuradas para “Forced Auth”, quando se altera o “System Authentication” de “None” para “EAP”, o estado da porta da estação passa para Down e em seguida volta para UP. Por isso deve-se tomar cuidado para não alterar este parâmetro em horário de produção.

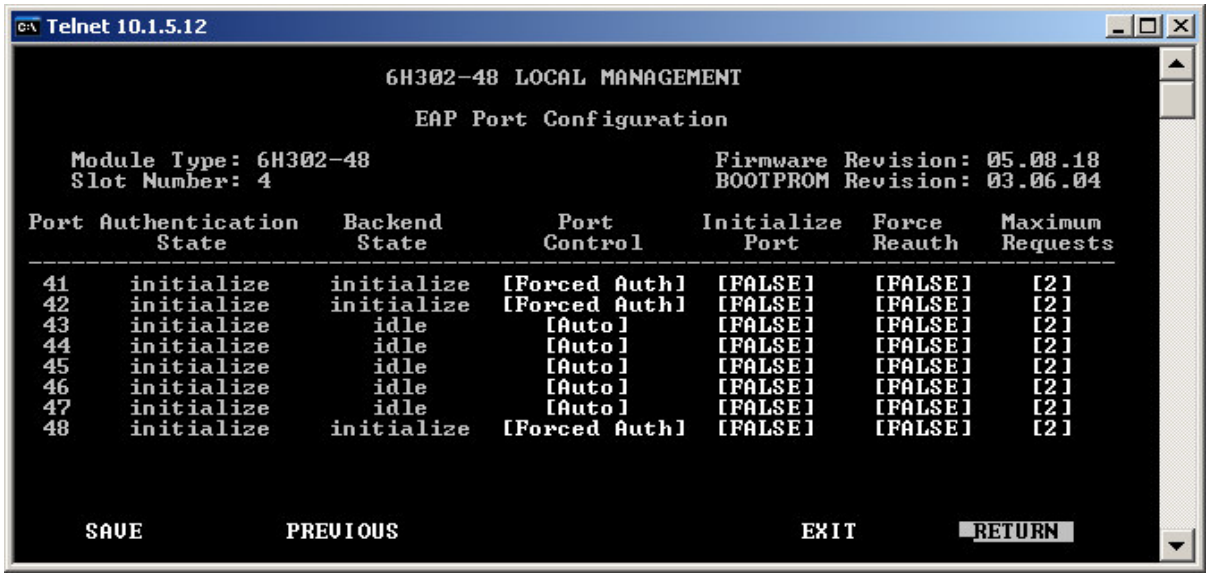


Figura 8 – Tela do switch 6H habilitando porta a porta o dot1x

3.2.2.4 Cisco 2950

Abaixo segue a seqüência de comandos que deve ser aplicada através do telnet no 2950 para se habilitar o dot1x.

Tabela 8 – Configurações do dot1x no switch Cisco 2950

aaa new-model	Habilita o AAA
aaa authentication dot1x default group radius	Cria um método de autenticação 802.1x configurado para o radius
dot1x system-auth-control	Habilita de forma global o 802.1x no switch
interface Fa0/1 dot1x port-control auto	Habilita a interface especifica para autenticação via 802.1x

3.2.3 Configuração dos parâmetros de controle de acesso por Mac Address

No caso de equipamentos como roteadores, switchs e impressoras de rede, podemos utilizar a autenticação por Mac Address, visto que nos mesmos não existe a possibilidade de configuração para autenticação via 802.1x.

3.2.3.1 Switch Enterasys B2 e 7H

Abaixo segue a seqüência de comandos que deve ser aplicada através do telnet no B2 e no 7H.

Tabela 9 – Configurações do controle de acesso por MAC nos switchs B2 e 7H

set maclock enable	Habilita de forma global no switch o método de autenticação por Mac address
set maclock enable fe.1.46	Habilita a autenticação por mac address em uma porta selecionada
set maclock firstarrival fe.1.46 0	Configura para apenas o MAC Address cadastrado funcionar na porta selecionada
set maclock 00:00:e2:4f:c1:50 fe.1.46 create	Informa o MAC Address permitido para funcionar na porta selecionada

Tabela 10 – Configurações adicionais do controle de acesso por MAC nos switchs B2 e 7H

set maclock disable	Desabilita de forma global no switch o método de autenticação por mac address
set maclock disable fe.1.46	Desabilita a autenticação por mac address em uma porta específica
clear maclock firstarrival fe.1.46	Volta a configuração original, onde é permitido que endereços mac address aprendidos acessem a rede
clear maclock 00:00:e2:4f:c1:50 fe.1.46	Retira um mac address cadastrado para uma porta específica

3.2.3.2 Switch Enterasys 6H

A autenticação por Mac Address no 6H funciona de forma diferenciada dos demais switchs. No momento em que o switch recebe o primeiro pacote da estação, estando habilitado a autenticação por Mac Address na porta específica, o switch envia uma requisição ao servidor radius configurado no switch, passando como parâmetro de usuário o endereço Mac Address e a senha que foi configurada no switch. Neste instante o servidor radius verifica no Active Directory, se existe um usuário criado no AD com o “username” igual ao MacAddress e com a mesma senha enviada pelo switch. Então o Active Directory responde ao servidor radius que por sua vez responde ao switch, que libera a porta de acesso ou não, dependendo do resultado da autorização.

Figura 9 – Tela do switch 6H onde configura a senha do “MAC authentication”

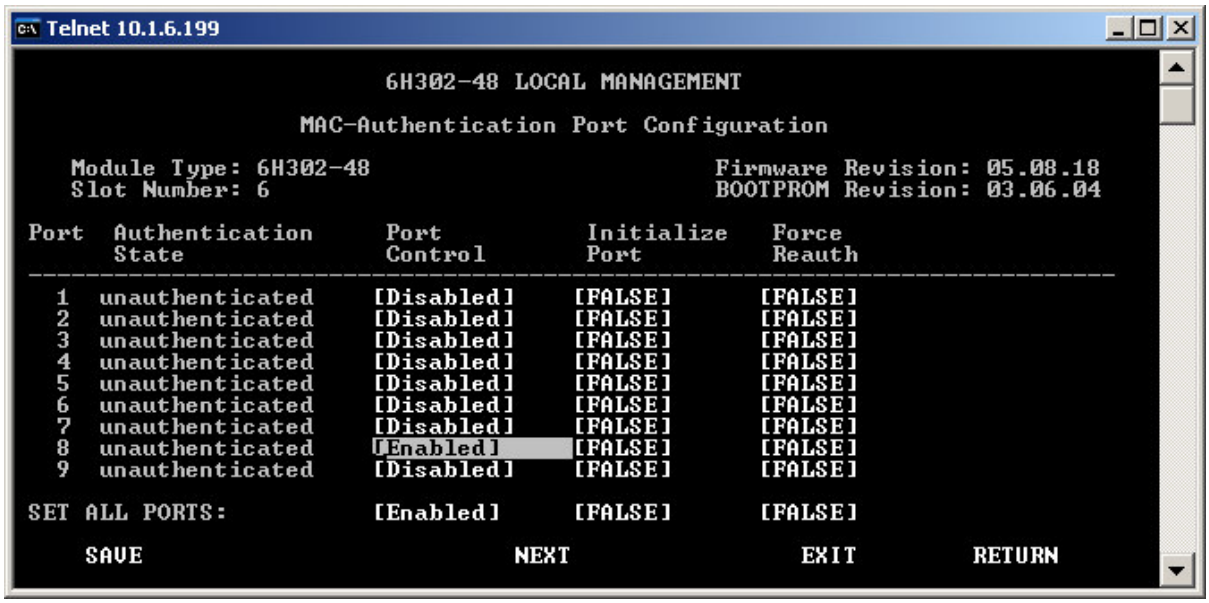


Figura 10 – Tela do switch 6H onde habilita a autenticação por MAC address na porta específica

3.2.3.3 Switch Cisco 2950

Abaixo segue a seqüência de comandos que deve ser aplicada através do telnet no 2950.

Tabela 11 – Configurações do controle de acesso por MAC no Cisco 2950

interface FastEthernet0/3	Porta 3 do switch
switchport mode access	Configura a interface para “mode access”, pois uma interface na configuração padrão (dynamic desirable) não pode ser configurada com uma porta segura
switchport port-security	Configura a porta para trabalhar em modo seguro
switchport port-security maximum 1	Configura o número de máximo de mac addresses que podem funcionar nesta porta
switchport port-security { violation protect | restrict | shutdown }	Configura qual será a ação tomada pelo switch se for violada a configuração aplicada na porta. Podem ser 3 opções: Protect – Pacotes de endereços mac não autorizados serão descartados Restrict – Incrementa um contador de segurança e envia um trap para a gerência Shutdown – Desabilita a porta
switchport port-security mac-address 000f.b0f4.e394	Configura o MAC Address permitido para funcionar na porta específicada

3.3 CONFIGURAÇÃO DO SERVIDOR

A função do servidor é de centralizar em uma base de dados (Active Directory) a gerência das contas dos usuários que tem permissão ou não para se autenticar no Switch. Mas para ser feita esta verificação, o switch se comunica com o servidor Radius que pode estar instalado no mesmo servidor onde está instalado o Active Directory. Como o PEAP necessita de uma chave pública para o servidor de autenticação, temos como pré-requisito a existência uma chave pública do Controlador de Domínio.

Desta forma, a configuração do servidor subdivide-se em duas partes.

- Configuração do Active Directory;
- Configuração do Radius

3.3.1 Configuração do Active Directory

A configuração “Store passwords using reversible encrytion” para todos os usuários no domínio fornece suporte para protocolos de aplicativo que exigem conhecimento da senha do usuário para propósitos de autenticação.

O uso da autenticação CHAP (Challenge Handshake Authentication Protocol) por meio de acesso remoto ou de serviços de Serviço de Autenticação da Internet

(IAS – Internet Authentication Service) exige que essa configuração de diretiva esteja ativada.

Segue abaixo o procedimento para esta configuração:

Entre no Active Directory Users and Computers e selecione “Properties”

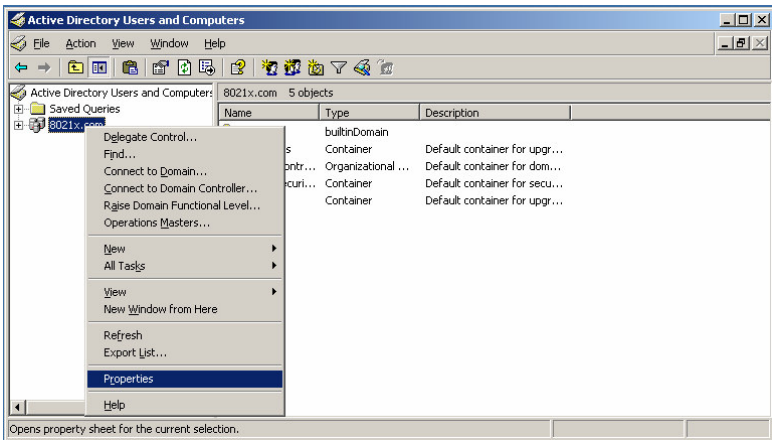


Figura 11 – Tela inicial do Active Directory abrindo as propriedades

Depois selecione “Group Policy” e clique no botão “Edit”

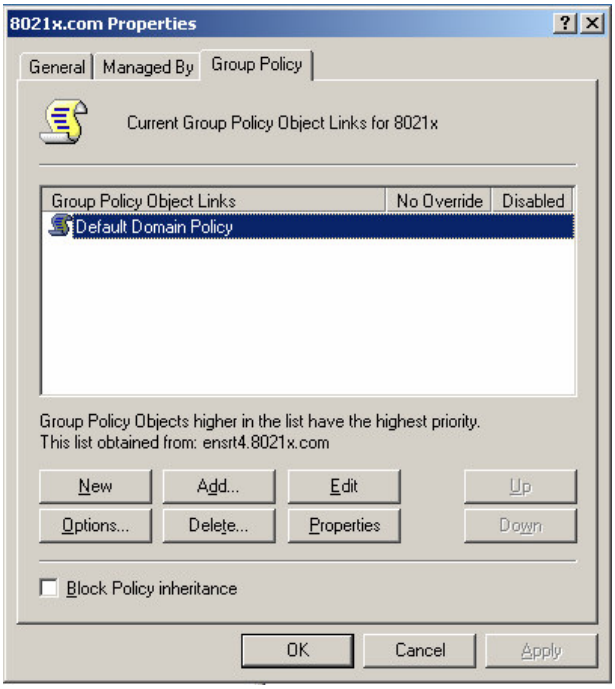


Figura 12 – Propriedades do Active Directory

Em seguida selecione:

“Computer Configuration\Windows Settings\Security Settings\Account Policies”

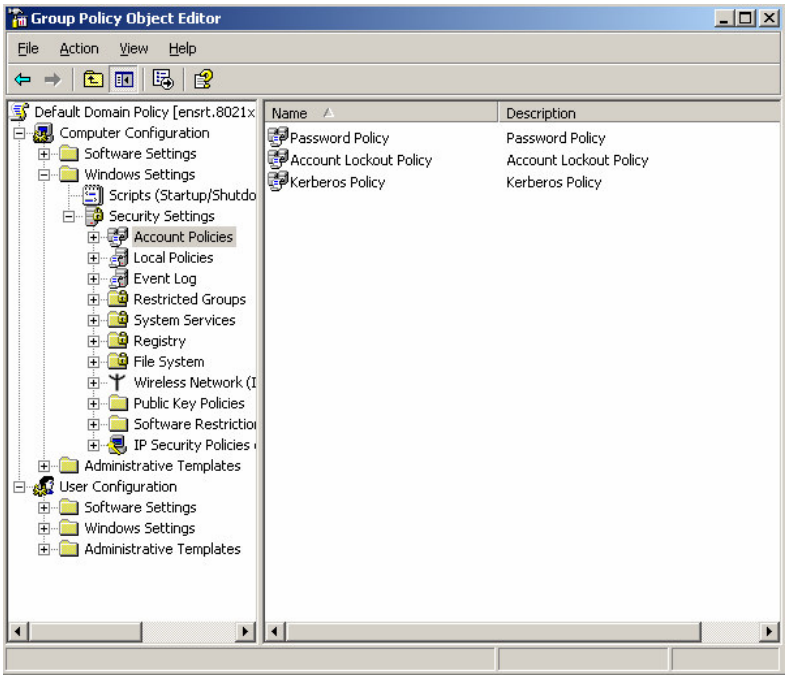


Figura 13 – Editor de políticas do Windows

Abra a pasta “Password Policy”

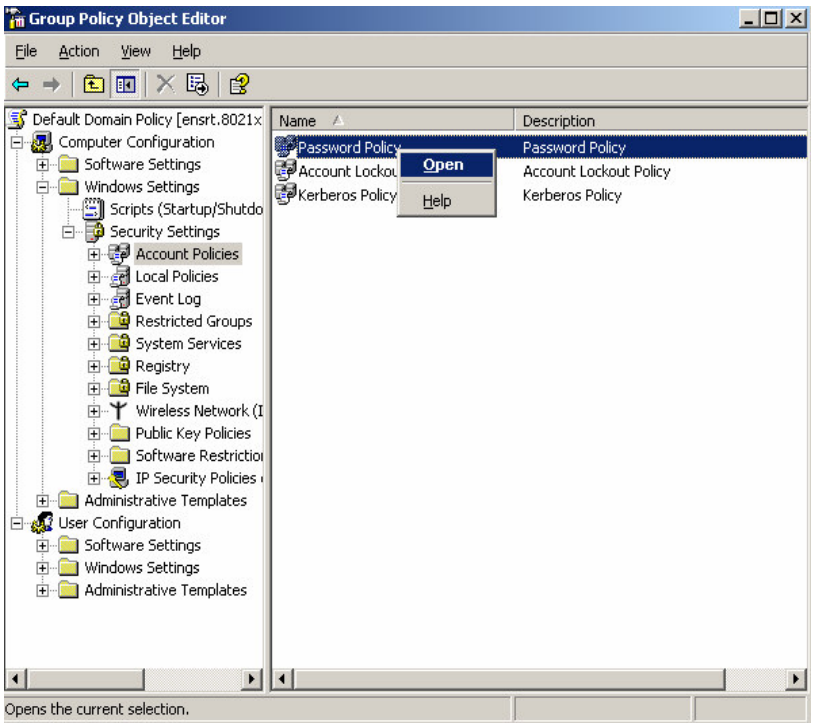


Figura 14 – Editor de políticas do Windows – Password Policy

Abra as propriedades de “Store passwords using reversible encryption”

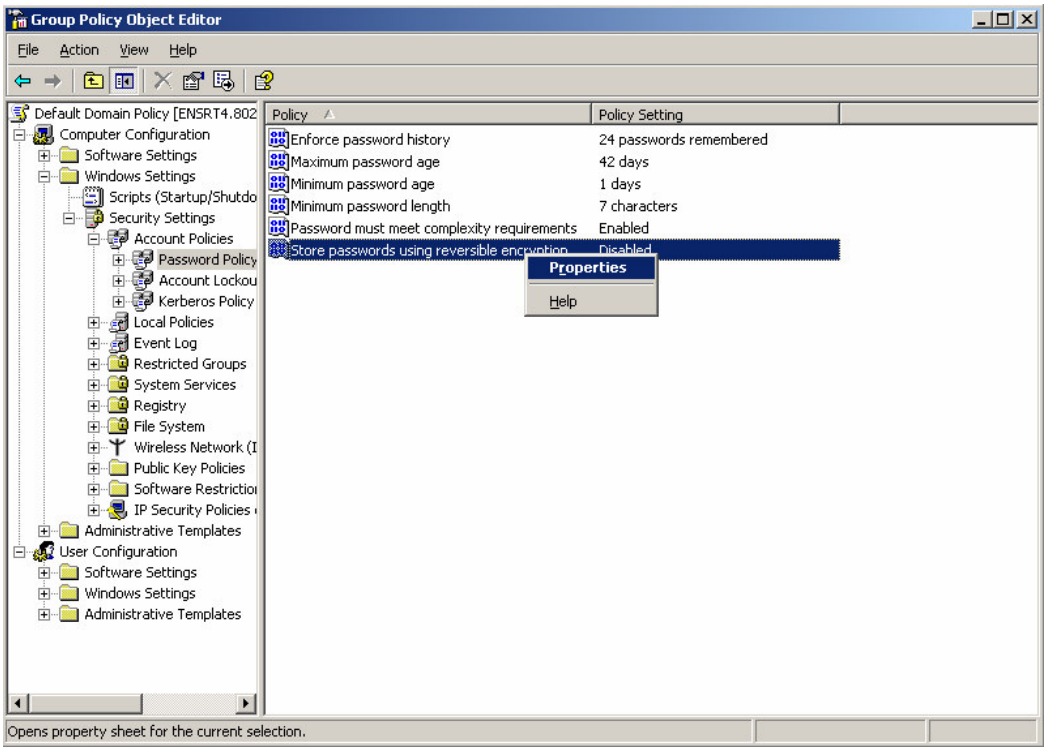


Figura 15 – Store password using encryption - Proprieties

Habilite esta opção e clique em “ok”

Figura 16 – Store password using encryption - Enabled

Após isso, é necessário configurar a propriedade “Remote Access Permission” das contas dos usuários no Active Directory que terão permissão para se autenticar. Esta configuração tem que ser feita usuário a usuário, conforme figura abaixo:

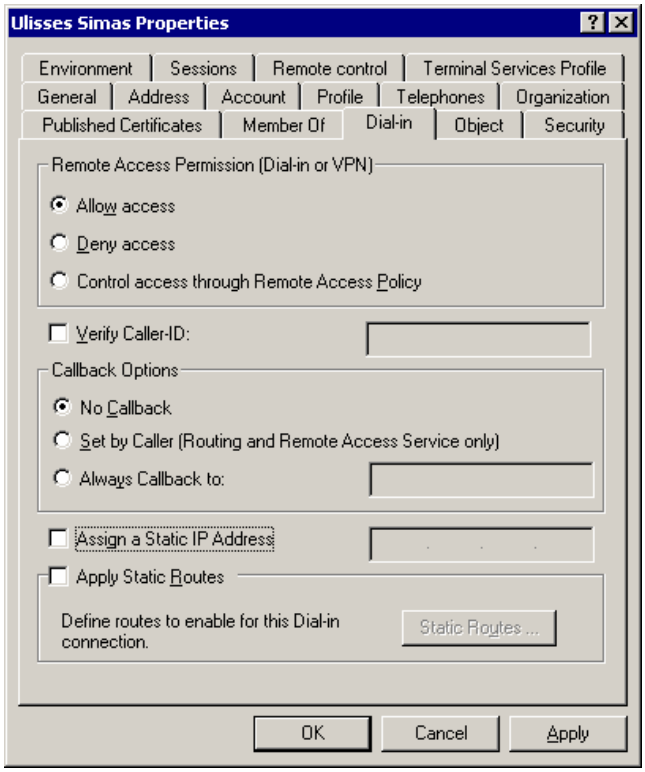


Figura 17 – Propriedades do usuário

3.3.2 Configuração do Internet Authentication Service (IAS - Radius)

3.3.2.1 Adicionando Clientes

É necessário que sejam cadastrados os IPs de gerência dos switchs que irão autenticar as suas respectivas portas de acesso. No caso do Windows Enterprise Edition e do Datacenter Edition, pode-se cadastrar o endereço da rede, ao invés de cadastrar cada IP de switch, conforme mostrada na tela de erro abaixo, onde tenta-se cadastrar um endereço de rede em um servidor Windows 2003 Standard.

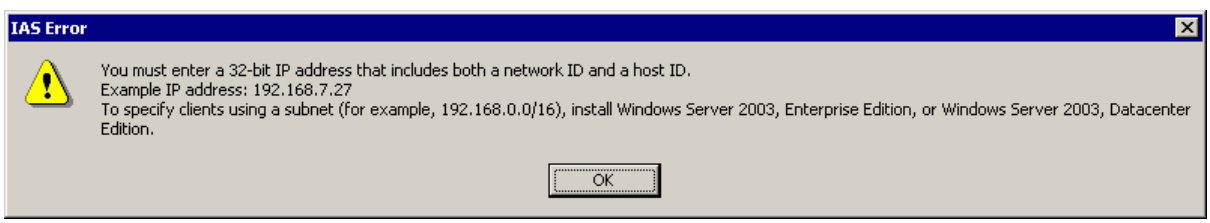


Figura 18 – Tela de erro do IAS

Na tela abaixo pode-se verificar todos os IPs que estão cadastrados.

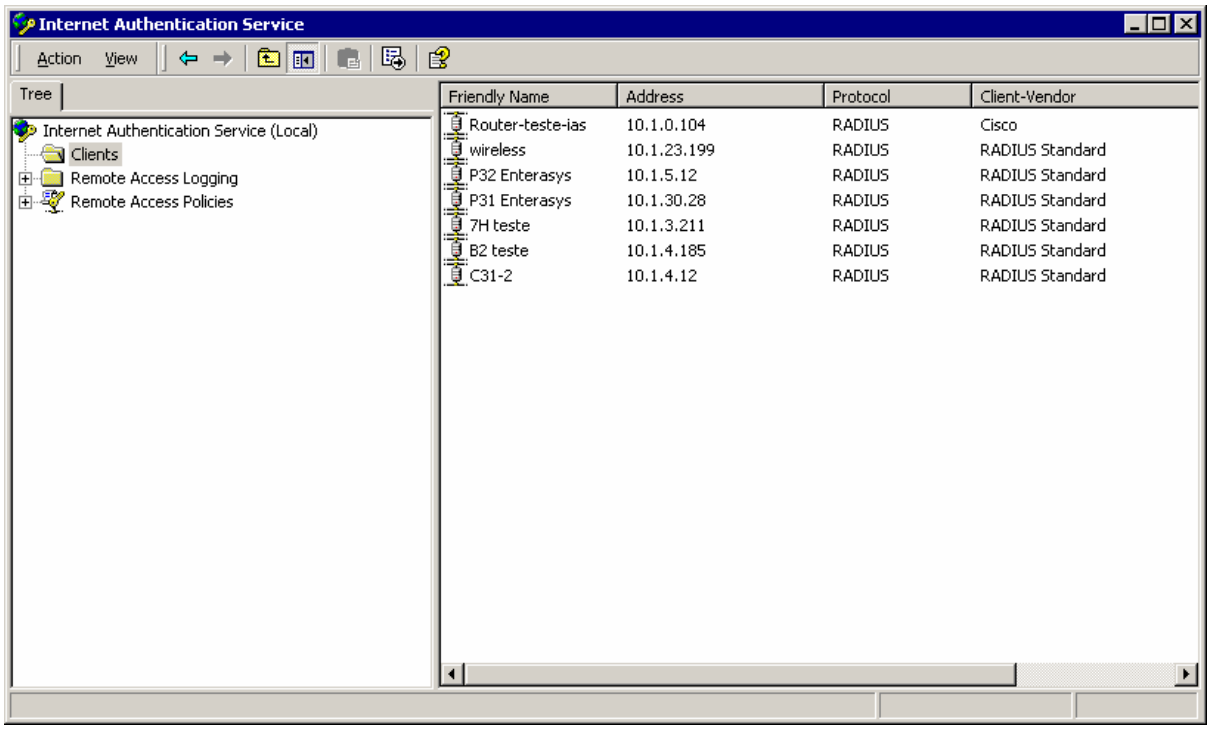


Figura 19 – Tela de clientes do IAS

Para se cadastrar um novo cliente, deve-se clicar com o botão direito do mouse em cima de “Clients” e selecionar “New RADIUS Client” e em seguida preencher os campos da tela conforme mostrado abaixo:

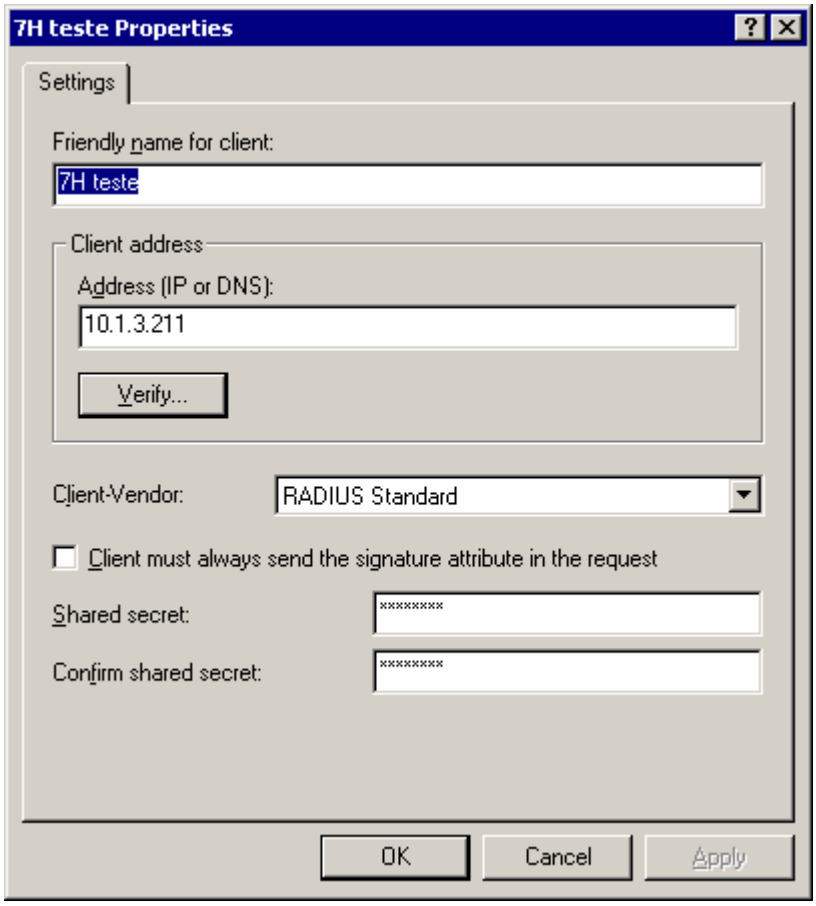


Figura 20 – Cadastramento de um novo cliente no IAS

Tabela 12 – Parâmentros de configuração de um novo cliente do IAS

Friendly name for client	Deve ser preenchido preferencialmente pelo hostname do equipamento que geralmente já é o nome pelo qual o switch é conhecido pelo administradores
Address (IP or DNS):	Endereço IP de gerência do switch
Client-Vendor	Se tiver o nome do fabricante na lista deve ser selecionado, porém não foi visto diferença ao selecioná-lo ou não
Shared secret	Frase secreta que será configurada no switch
Confirm shared secret	Confirmação da frase secreta que será configurada no switch

3.3.2.2 Configurando Políticas

As políticas são uma seqüência de regras que definem como as conexões são autorizadas ou rejeitadas. Essas regras podem ser usadas para autenticação de conexões de telnet, VPN ou 802.1x.

Na tela abaixo pode-se verificar todas as políticas que estão cadastradas no IAS.

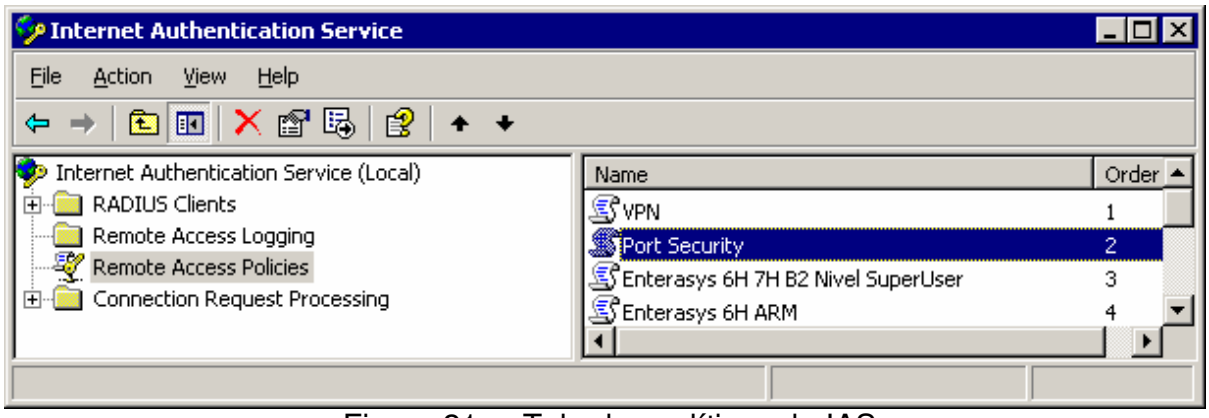


Figura 21 – Tela das políticas do IAS

Nesta tela são apresentadas 4 políticas:

- VPN – validação dos usuários que acessam a VPN externa
- Port Security – validação dos usuários/portas dos switchs com 802.1x habilitados
- Enterasys 6H ... – validação do telnet/ssh para gerência dos equipamentos

No caso do nosso estudo, entraremos em detalhe na política “Port Security”, detalhando as telas de configuração:

Para verificarmos a configuração de uma política já definida, bastar dar um duplo clique em cima do nome da política, conforme ilustrada na Figura 20.

As condições desta política são que o usuário que esteja se logando seja integrante do grupo “Port Security” do domínio INFRAW2K3 e que o tipo de porta seja igual a Ethernet. Foi incluída o NAS-Port-Type, para diferenciar a solicitação de uma autenticação de Telnet ou VPN desta autenticação, pois existem usuários que tem permissão nas três políticas definidas e que devem receber “strings” de configurações diferentes para cada caso. Então o NAS-Port-Type serve para diferenciar o tipo de solicitação feita pelo switch ao servidor radius. Esta configuração está ilustrada na Figura 22.

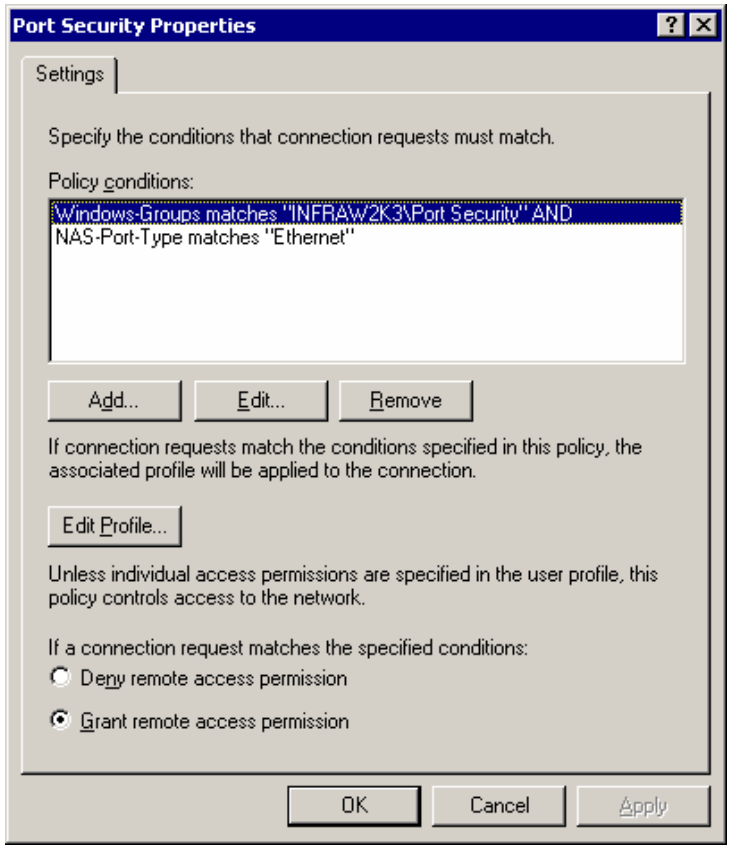


Figura 22 – Tela de propriedades da política do IAS

Para verificarmos outras configurações, devemos clicar no botão “Edit Profile”

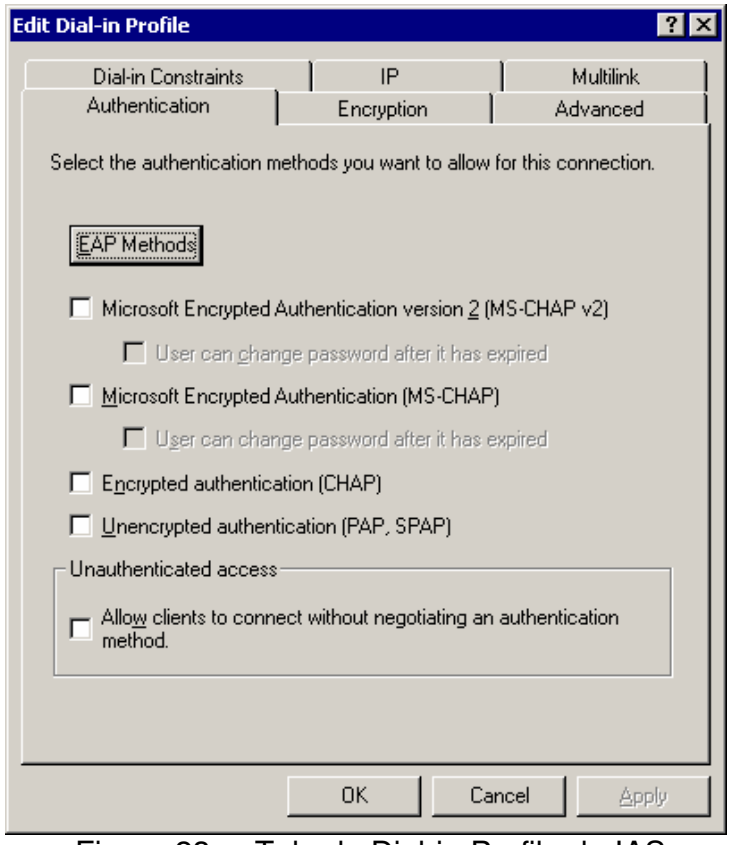


Figura 23 – Tela do Dial-in Profile do IAS

E depois clicar no botão “EAP Methods” para ter acesso às configurações EAP e MD5.

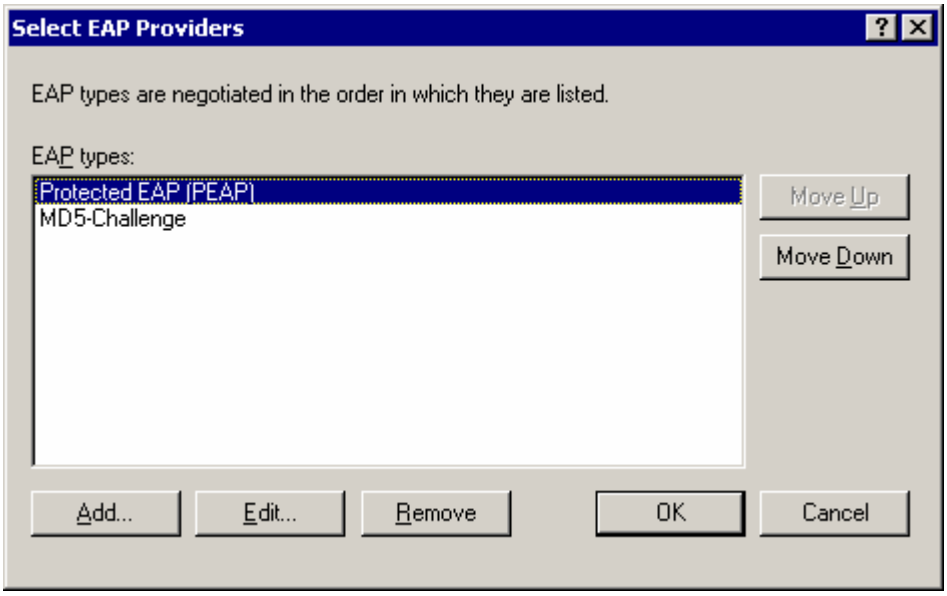


Figura 24 - Tela de configuração dos Métodos EAP

3.3.2.2.1 Política PEAP

Esta política é utilizada pelas estações dos usuários que estão no domínio da empresa, onde será utilizada a mesma autenticação do Windows para autenticar na porta do switch. Ao clicar no botão “Edit”, aparece outras opções de configuração conforme a Figura 25.

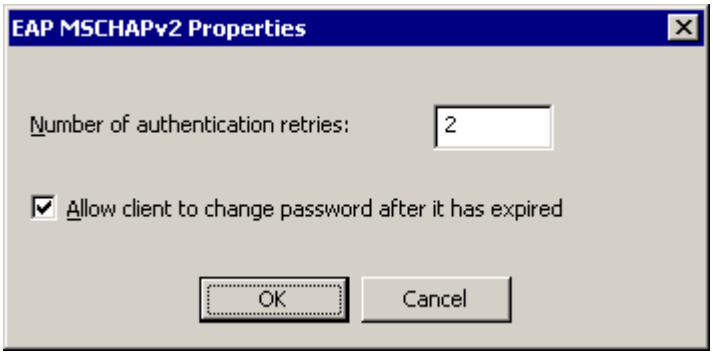


Figura 25 - Tela de configuração adicional do PEAP

3.3.2.2.2 Política MD5

Esta política é utilizada por estações de trabalho que não estão no domínio, como por exemplo, consultores externos. Dessa forma, o consultor irá se logar localmente em sua estação de trabalho e depois irá se autenticar na rede, como será

demonstrado no próximo capítulo. Esta configuração não requer nenhuma configuração adicional depois de incluí-la na tela do EAP Providers.

3.4 CONFIGURAÇÃO DA ESTAÇÃO DE TRABALHO

3.4.1 Configurando estação para a política PEAP

Abaixo segue a seqüência de telas para configurar o Windows XP, fazendo este parte do domínio da empresa, para autenticar no switch utilizando a mesma conta de usuário que se loga no domínio.

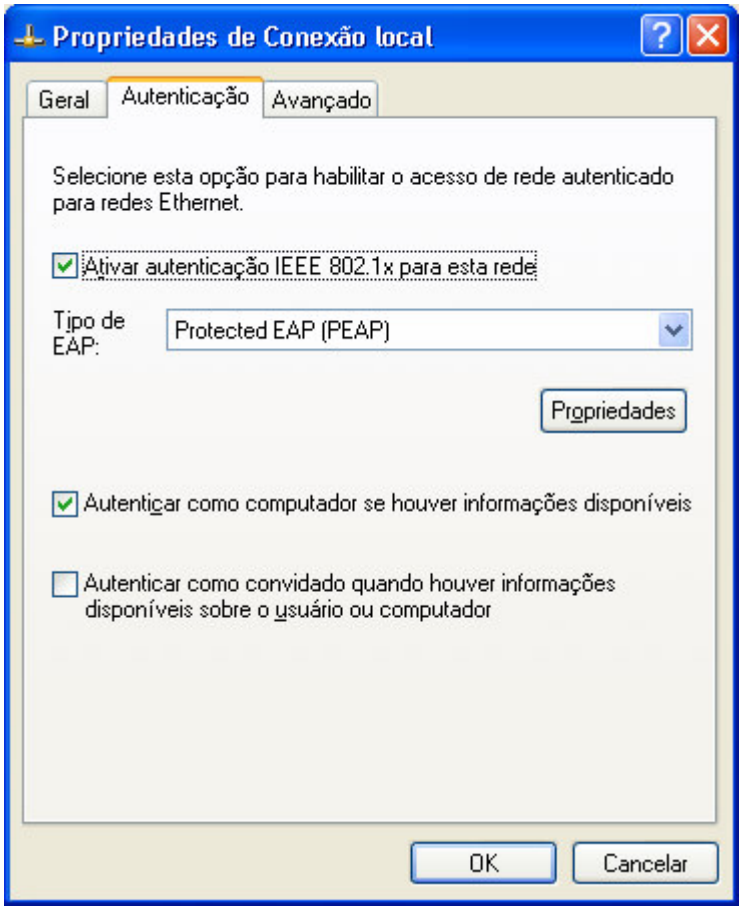


Figura 26 - Tela “Propriedades de Conexão local” – aba Autenticação

Marcar a opção “Ativar autenticação IEEE 802.1x para esta rede”, selecionar a opção “Tipo de EAP” como “Protected EAP (PEAP)” e marcar “Autenticar como computador se houver informações disponíveis”.

É muito importante que seja marcada a opção de “Autenticar como computador ...”, pois o Windows XP, no momento em que solicita o nome e a senha do usuário, necessita que a placa de rede já esteja ativa, pois caso contrário, o

Windows dará a mensagem que o controlador de domínio não pode ser encontrado, pois a autenticação do Windows funciona da seguinte maneira:

Ao ligar a estação, a mesma será autenticada no switch, através da conta da estação que existe no Active Directory. Mas para que isto ocorra, é necessário incluir ao grupo do Active Directory que libera o acesso através do servidor radius, a conta da estação. Então ao aparecer à tela de login do Windows, a placa de rede já estará ativa. E após o usuário entrar com o seu usuário e senha, o Windows irá autenticá-lo no domínio e em seguida autenticá-lo no switch (802.1x) através da conta do usuário, habilitando ou não a porta do switch, dependendo da resposta do servidor radius ao switch.

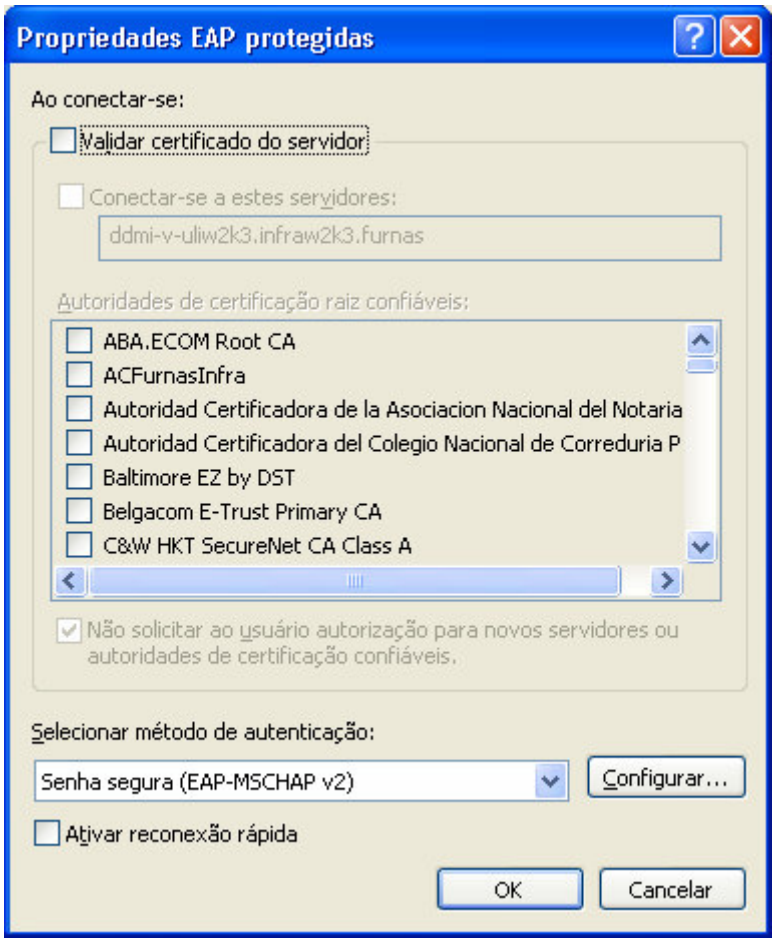


Figura 27 - Tela “Propriedades EAP Protegidas”

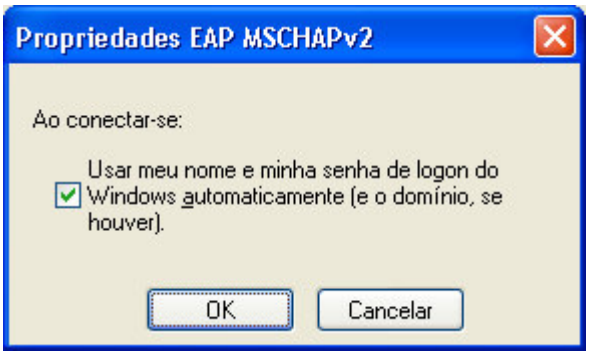


Figura 28 - Tela “Propriedades EAP MSCHAPv2”

3.4.2 Captura de pacotes entre o Switch e o Servidor Radius (PEAP)

Abaixo é mostrada a captura dos pacotes pelo analisador de protocolo Ethereal, mostrando a troca de pacotes entre o switch e o servidor radius. São trocados diversos pacotes entre o switch e o servidor radius, pois quando é utilizado PEAP, é necessário que o servidor tenha uma chave pública de certificado digital que é utilizada para criar um túnel encriptografado entre o switch e o servidor radius, protegendo as informações utilizadas na autenticação sejam inspecionadas por algum “sniffer”.

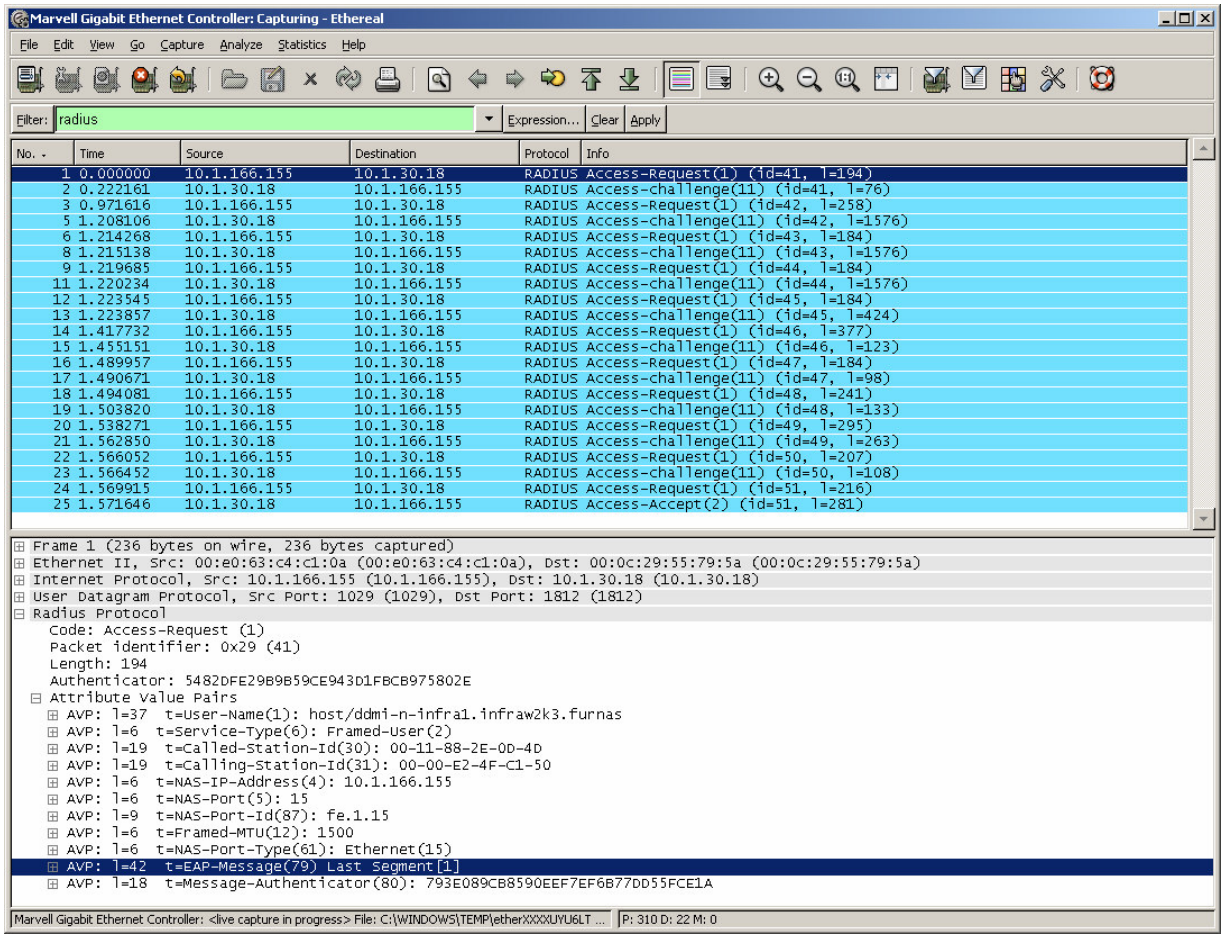


Figura 29 - Tela do Ethereal com captura da requisição da estação (PEAP)

Esta tela mostra o request do switch com o IP de origem 10.1.166.155 ao servidor radius 10.1.30.18 e diversos parâmetros que são passados como, por exemplo: Nome do domínio\noma da estação (INFRA\ddmi-n-infra1.infraw2k3.furnas), endereço MAC do switch (00-11-88-2E-0D-4D), endereço MAC da estação que está se conectando ao switch (00-00-E2-48-32-0D), endereço ip do switch (10.1.166.155), porta do switch (3). Como explicado anteriormente, esta sequência de pacotes está fazendo a autenticação da estação de trabalho no momento em que aparece a tela de login do Windows XP, e por isso é passado como “User-name” o nome da estação..

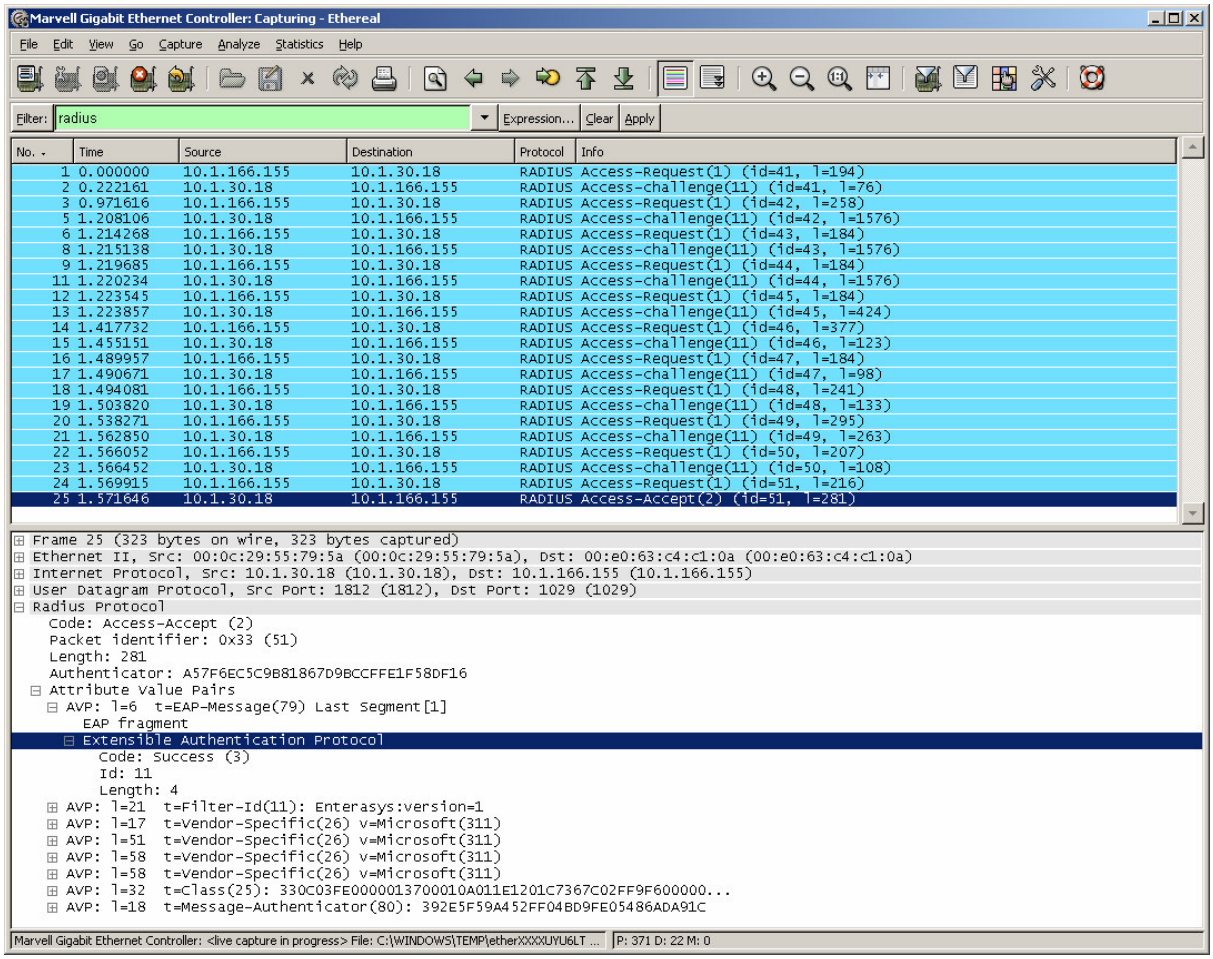


Figura 30 - Tela do Ethereal com captura do aceite da estação (PEAP)

Esta tela mostra o aceite com sucesso pelo servidor radius ao switch. Neste instante o switch deixa a porta com status de “Up” e passa a fazer o “forwarding” dos pacotes.

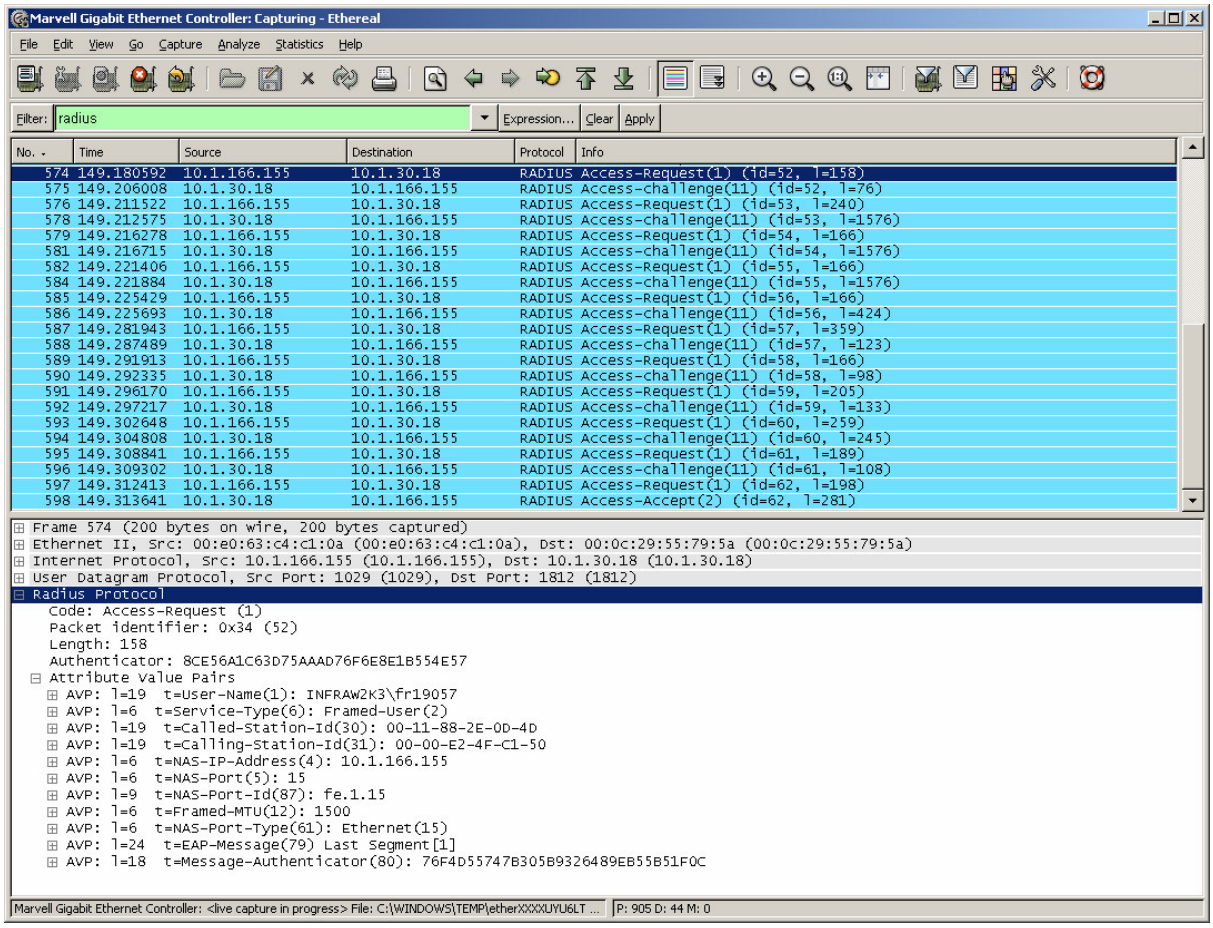


Figura 31 - Tela do Ethereal com captura da requisição do usuário (PEAP)

Após entrarmos com o usuário e senha na tela de login do Windows, como a porta está em “Up”, é feita o login do Windows no controlador de domínio e ao mesmo tempo é feita uma nova autenticação da porta do switch, como mostrado na tela acima. A diferença deste request para o mostrado na figura acima é que o parâmetro User-Name que agora é uma conta de usuário do Active Directory, e não uma conta de computador.

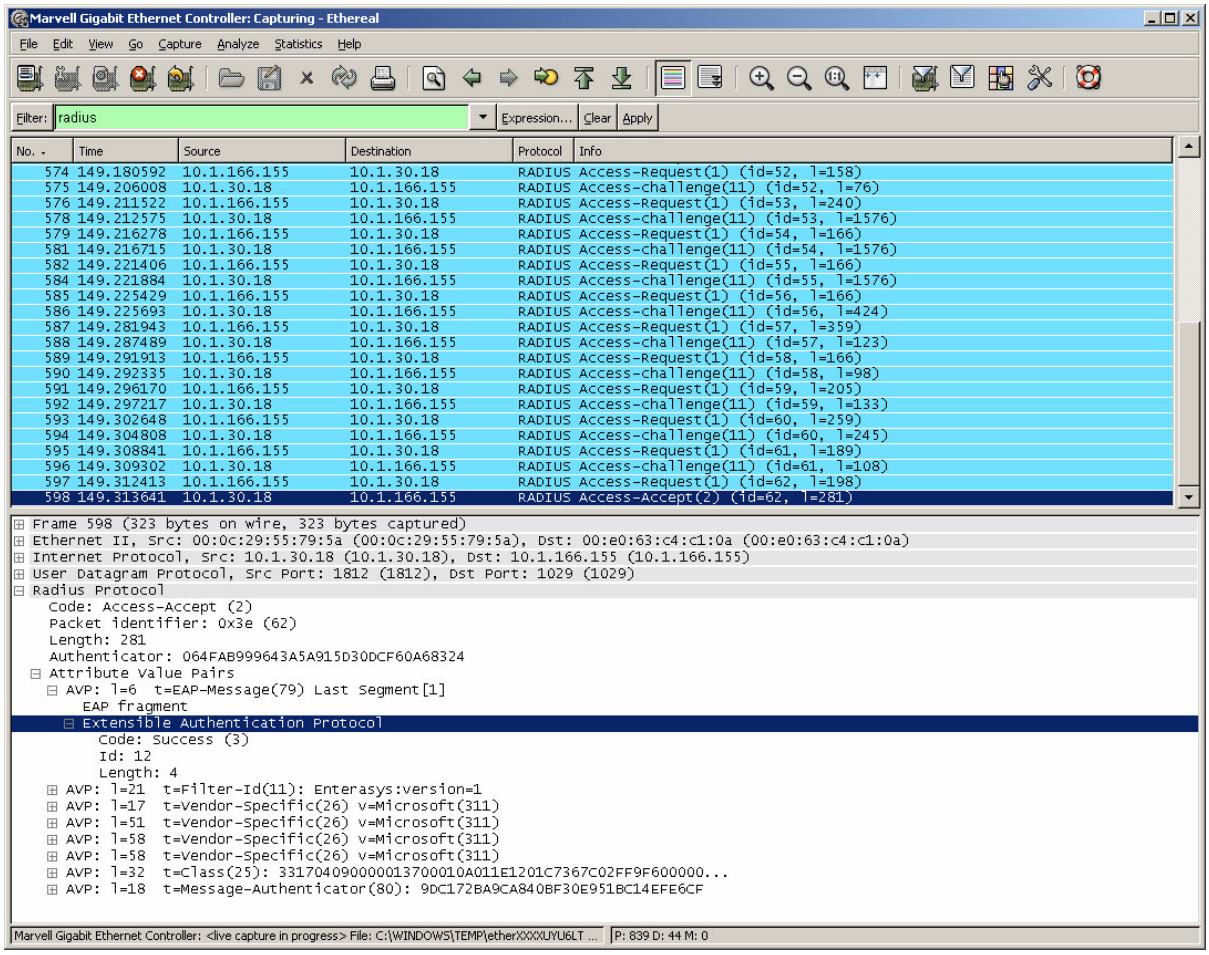


Figura 32 - Tela do Ethereal com captura do aceite do usuário (PEAP)

Esta tela mostra novamente aceite com sucesso pelo servidor radius ao switch, deixando o mesmo a porta com status de “Up” e fazendo o “forwarding” dos pacotes recebidos.

3.4.3 Configurando estação para a política MD5

Esta política é utilizada por estações de trabalho que não estão no domínio, como por exemplo, consultores externos. Dessa forma, o consultor irá se logar localmente em sua máquina e depois irá se autenticar na rede.

Para configurar a estação que não está no domínio deve seguir os seguintes passos:

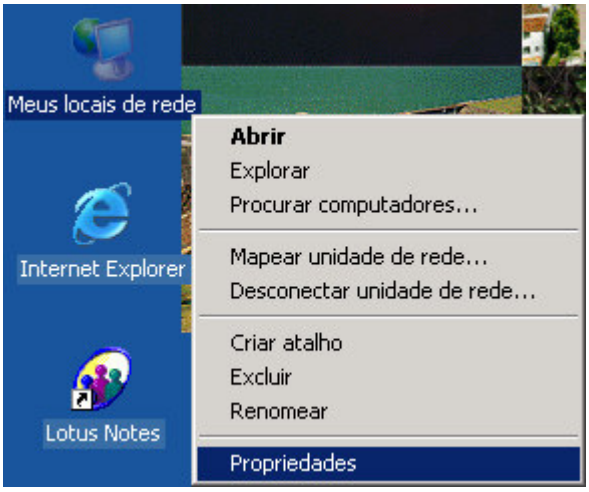


Figura 33 - Tela do menu do ícone “Meus locais de rede”

Clicar com o botão direito do mouse em cima de “Meus locais de rede” e selecionar “Propriedades”

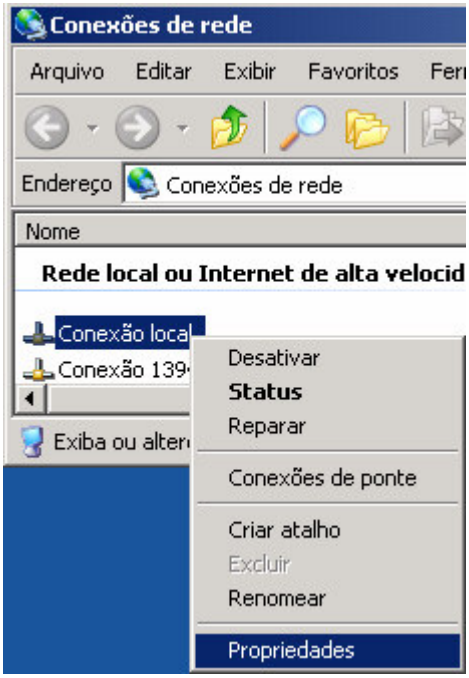


Figura 34 - Tela do menu da “Conexão local”

Clicar com o botão direto do mouse em cima da conexão de rede local ativa e selecionar “Propriedades”

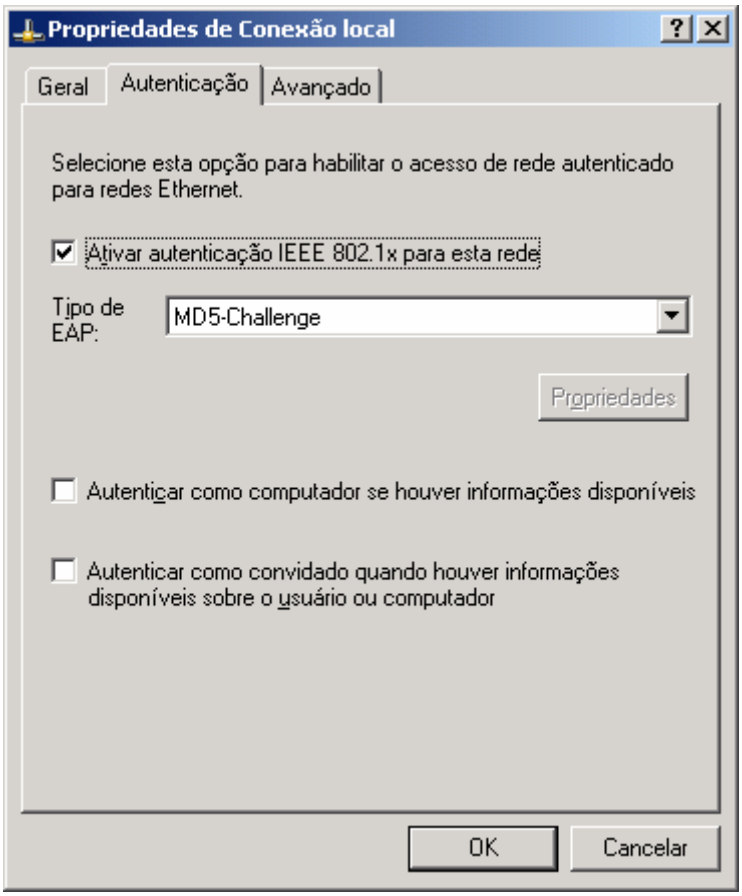


Figura 35 - Tela das “Propriedades de Conexão local”

Selecionar a aba Autenticação e marcar a opção “Ativar autenticação ...” e em seguida selecionar o Tipo de EAP para “MD5-Challenge”

Depois de feita a configuração acima, a placa de rede só estará ativa e com ip válido depois que for feita a autenticação na porta de acesso do switch. Para isto deve-se dar um duplo clique na mensagem que aparecerá conforme a figura abaixo.

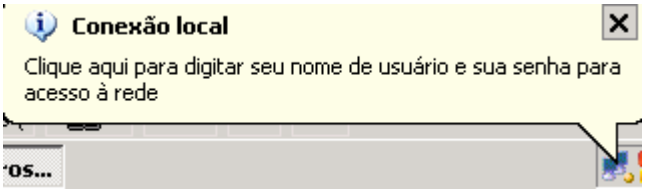


Figura 36 - Tela de solicitação de autenticação da “Conexão local”

Logo em seguida, aparecerá a tela de login solicitando o nome do usuário, a senha e o nome do domínio, que efetuando a autenticação com sucesso o switch

liberará a porta do switch para que a estação de trabalho tenha acesso aos recursos da rede.

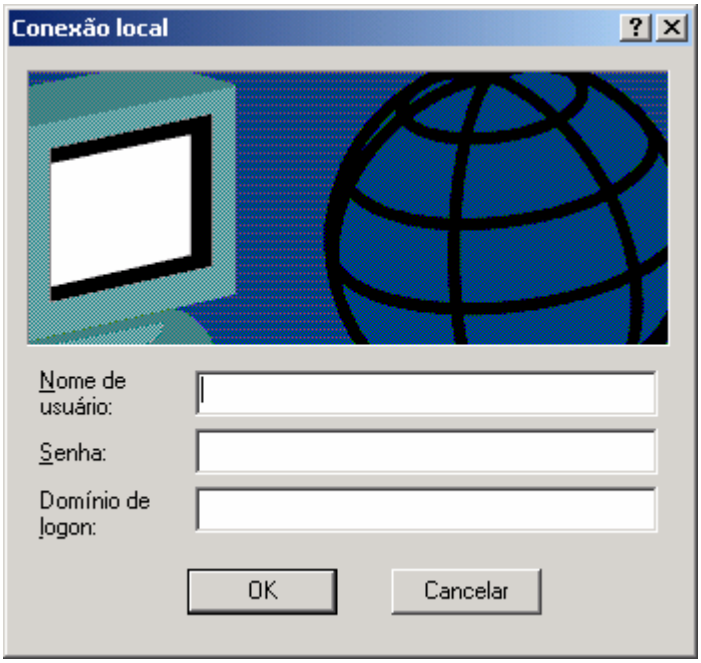


Figura 37 - Tela de solicitação de usuário, senha e domínio da “Conexão local”

3.4.4 Captura de pacotes entre o Switch e o Servidor Radius (MD5)

Abaixo é mostrada a captura dos pacotes pelo analisador de protocolo Ethereal, mostrando a troca de pacotes entre o switch e o servidor radius. São trocados quatro pacotes entre os mesmos conforme as ilustrações abaixos e suas respectivas explicações:

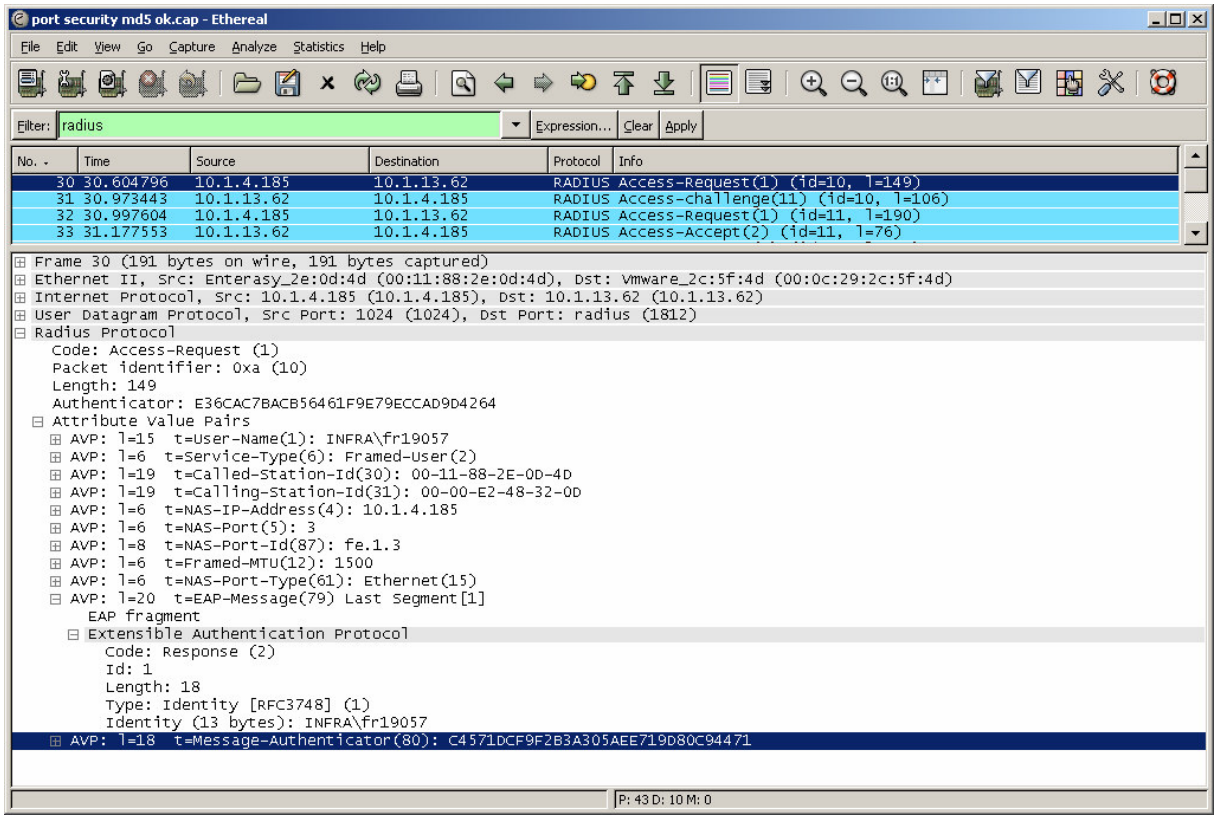


Figura 38 - Tela do Ethereal com captura da requisição da estação (MD5)

Esta tela mostra o request do switch com o IP de origem 10.1.4.185 ao servidor radius 10.1.13.62 e diversos parâmetros que são passados como, por exemplo: Nome do domínio\usuário (INFRA\fr19057), endereço MAC do switch (00-11-88-2E-0D-4D), endereço MAC da estação que está se conectando ao switch (00-00-E2-48-32-0D), endereço ip do switch (10.1.4.185), porta do switch (3).

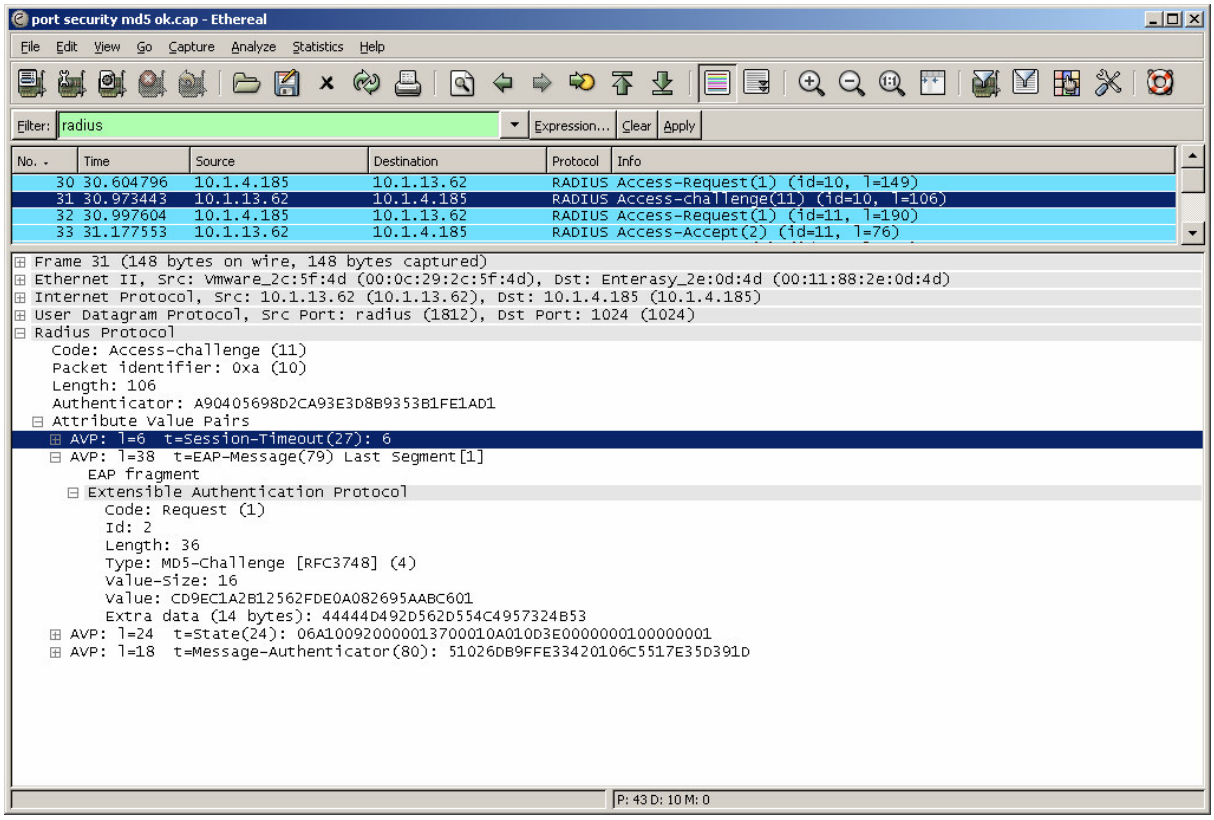


Figura 39 - Tela do Ethereal com envio do desafio (MD5)

Esta tela mostra a resposta do servidor radius à solicitação feita pela switch. Neste instante o servidor radius envia o desafio (challenge) ao switch para verificar a senha.

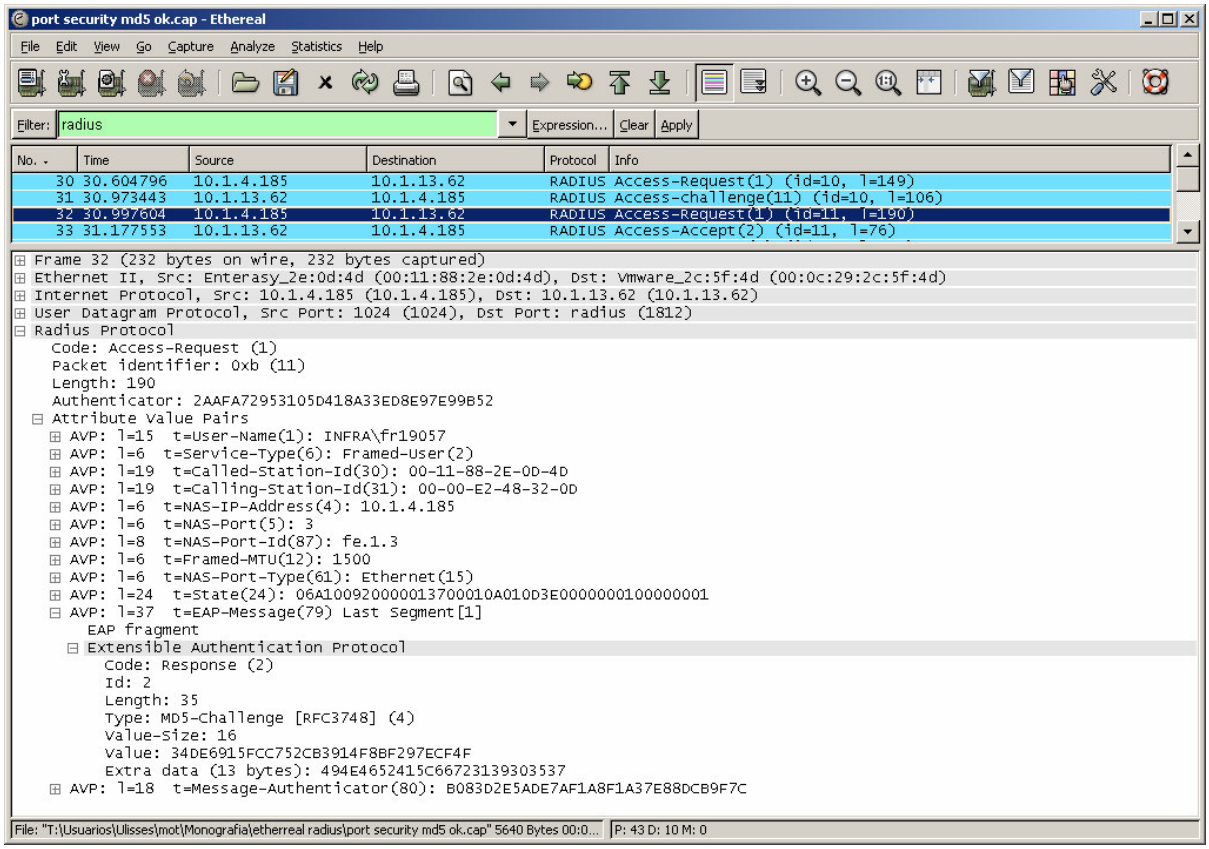


Figura 40 - Tela do Ethereal com envio da resposta do desafio (MD5)

Esta tela mostra a resposta do switch à solicitação feita pelo servidor radius. Neste instante o switch envia a resposta do desafio (challenge) ao servidor radius para verificar a senha.

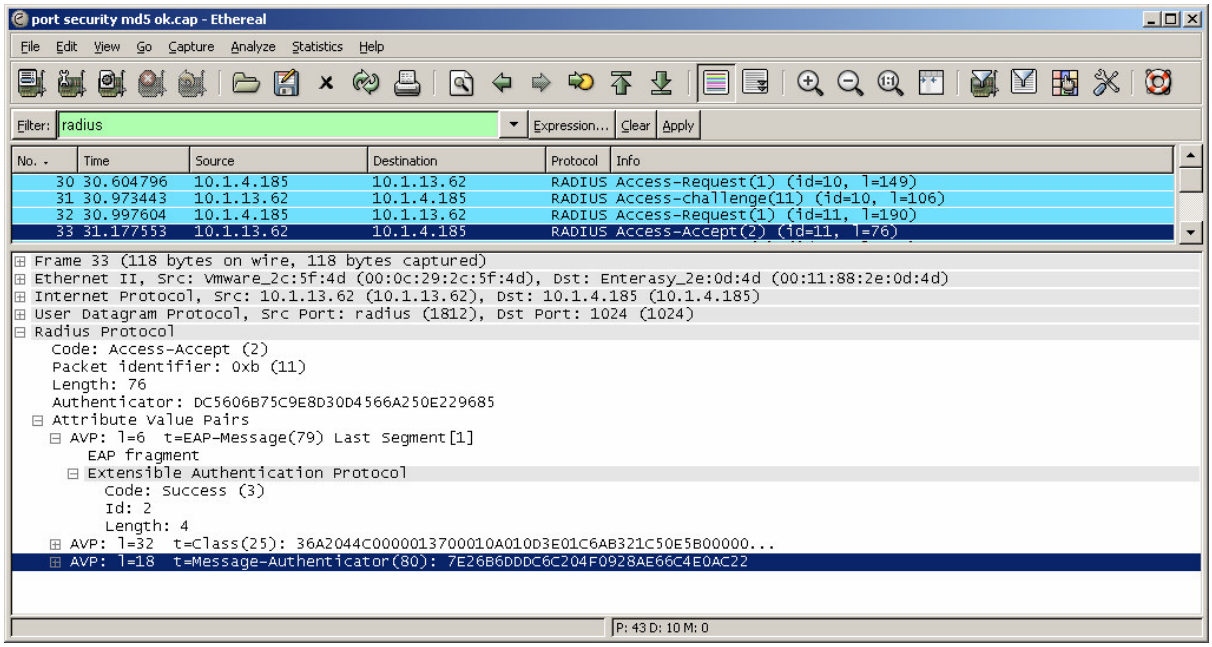


Figura 41 - Tela do Ethereal com aceite da requisição (MD5)

Esta tela mostra o aceite com sucesso pelo servidor radius ao switch.

4 CONCLUSÃO

4.1 CONTRIBUIÇÕES

Temos como principais contribuições desta pesquisa a documentação das configurações dos switchs e servidores para se ter uma rede segura utilizando as funcionalidades existentes nestes equipamento utilizando o padrão IEEE 802.1x. Além disso, foram citados casos práticos de problemas encontrados na implementação destas configurações que servem de exemplo para quando outras pessoas vierem a implementar estas configurações em seus equipamentos, e assim, já tenham em mente ter seus firmwares atualizados.

4.2 TRABALHOS FUTUROS

Como trabalhos futuros e complementar a esta pesquisa, temos em mente descrever a configuração das estações Windows XP de forma automatizada, visto que em grandes empresas temos um número grande de estações e estudar a integração das políticas de segurança de acesso a rede em conjunto com as políticas de anti-vírus e paths de segurança instalados nas estações, liberando o acesso a rede somente se estes itens estiverem atualizados e ativos.

REFERÊNCIAS

WIKIPÉDIA, HUB. **Concentrador**. Disponível em http://pt.wikipedia.org/wiki/Concentrador. Acesso em 05 abr. 2006.

WIKIPÉDIA, SWITCH. **Comutador (Redes)**. Disponível em http://pt.wikipedia.org/wiki/Switch. Acesso em 05 abr. 2006.

WIKIPÉDIA, WINDOWS 3.X. **Windows 3.x**. Disponível em http://pt.wikipedia.org/wiki/Windows_3.x. Acesso em 05 abr. 2006.

WIKIPÉDIA, WINDOWS 98. **Windows 98**. Disponível em http://pt.wikipedia.org/wiki/Windows_98. Acesso em 05 abr. 2006.

WIKIPÉDIA, WINDOWS NT. **Microsoft Windows**. Disponível em http://pt.wikipedia.org/wiki/Windows#Windows_NT. Acesso em 05 abr. 2006.

WIKIPÉDIA, WINDOWS XP. **Windows XP**. Disponível em http://pt.wikipedia.org/wiki/Windows_XP. Acesso em 05 abr. 2006.

WIKIPÉDIA, WINDOWS 2003. **Windows Server 2003**. Disponível em http://pt.wikipedia.org/wiki/Windows_Server_2003. Acesso em 05 abr. 2006.

MICROSOFT, AD. **Descrição Geral do Active Directory**. Disponível em http://www.microsoft.com/technet/prodtechnol/windowsserver2003/pt-pt/library/ServerHelp/7c981583-cf41-4e6c-b1f6-5b8863475ede.mspx?mfr=true. Acesso em 25 mai. 2006.

MICROSOFT, RADIUS. **Protocolo RADIUS**. Disponível em http://www.microsoft.com/technet/prodtechnol/windowsserver2003/pt-br/library/ServerHelp/9ecf38e5-3200-490d-83d8-2c624da94d8b.mspx?mfr=true. Acesso em 25 mai. 2006

MICROSOFT, EAP. **Protocolo de autenticação extensível (EAP, Extensible Authentication Protocol)**. Disponível em http://www.microsoft.com/technet/prodtechnol/windowsserver2003/pt-pt/library/ServerHelp/a42b4d9e-0965-4bcc-99bd-918642886e50.mspx?mfr=true. Acesso em 25 mai. 2006.

MICROSOFT, 802.1x. **Gerenciamento de Segurança - Agosto de 2005)**. Disponível em http://www.microsoft.com/brasil/technet/seguranca/colunas/sm0805.mspx. Acesso em 12 dez. 2006.